A tripartite model of trust in Facebook : acceptance of information personalization, privacy concern, and privacy literacy

Rosenthal, Sonny; Wasenden, Ole-Christian; Gronnevet, Gorm-Andreas; Ling, Rich

2019

Rosenthal, S., Wasenden, O.-C., Gronnevet, G.-A., & Ling, R. (2020). A tripartite model of trust in Facebook : acceptance of information personalization, privacy concern, and privacy literacy. Media Psychology, 23(6), 840-864. doi:10.1080/15213269.2019.1648218

https://hdl.handle.net/10356/145658

https://doi.org/10.1080/15213269.2019.1648218

A Tripartite Model of Trust in Facebook:

Acceptance of Information Personalization, Privacy Concern, and Privacy Literacy

Sonny Rosenthal[1]

Ole-Christian Wasenden[2]

Gorm-Andreas Gronnevet[2]

Rich Ling[1]

[1]Wee Kim Wee School of Communication and Information,

Nanyang Technological University, Singapore

[2]Telnor Research, Telnor Group

Corresponding author: Please address correspondence to the lead author at sonnyrosenthal@ntu.edu.sg, +65 6790 4070.

Note. This is a pre-publication version. The final version appears in *Media Psychology* and is available at https://doi.org/10.1080/15213269.2019.1648218.

Abstract

This study draws on the mental accounting perspective and a tripartite model of trust to explain why users trust Facebook. We argue that trust in Facebook is related to (1) trust in companies that collect personal data, (2) acceptance of information personalization, (3) low privacy concern, and (4) low privacy literacy. Further, we argue that privacy literacy amplifies the relationship between privacy concern and the other factors. This is because, among individuals with high privacy literacy, privacy concern is especially diagnostic of the potential harms of a loss of privacy. These arguments align broadly with theorizations about factors influencing privacy-related cognitions. We analyzed cross-national survey data from 4,684 mobile internet users and found support for our predictions. Our findings suggest that privacy concern has a weak relationship with trust-related beliefs except for among individuals with good privacy literacy. Among those individuals, privacy concern is negatively related to trust, potentially threatening an important revenue stream to data-driven companies, especially amid growing calls for privacy literacy education.

Keywords: trust; Facebook; privacy literacy; privacy concern; personalization

A Tripartite Model of Trust in Facebook:
Acceptance of Information Personalization, Privacy Concern, and Privacy Literacy

Message tailoring in social media became the focus of public scrutiny early in 2018 when news reports surfaced of a massive data breach at Facebook (e.g., Badshah, 2018). The breach was newsworthy because of its scale, affecting tens of millions of users; because it violated the trust those users put in Facebook to safeguard their personal data; and because a political consulting firm used their data to target political messages that may have influenced the outcome of the 2016 United States presidential election. In September 2018, Facebook had to deal with another large-scale breach when hackers gained access to the personal data of 29 million users (Barrett, 2018). Those data included things like name and email address and, for some affected users, more personal information like hometown, educational background, and the most recent places they checked in. Both breaches had to do with how users shared their personal data and how third parties used those data inappropriately.

An interesting question is why, given the vulnerability of the system, Facebook users shared their personal information. Research on this apparent privacy paradox has offered many different explanations that are often context-specific (Kokolakis, 2017). In the context of Facebook use, one explanation is that users trusted Facebook to protect their privacy (Beldad & Hegner, 2017). Although the recent scandals have eroded user trust in Facebook (O'Flaherty, 2018), it is worthwhile examining some of the beliefs and, perhaps, misperceptions that underlie user trust. The current study builds on Park, Campbell, and Kwak (2012), who proposed a tripartite model to explain privacy protection behaviors. It considers the effects of trust in data institutions, acceptance of message personalization, general privacy concern, and privacy literacy. Whereas Park et al. (2012) examined similar concepts as predictors of privacy

protection, the current study examines how those concepts are related directly to trust. Understanding how individuals form trusting beliefs can explain not only privacy control behaviors, but also information sharing behaviors and a host of other activities that may affect the privacy of social media users. We examine this basis of trust by analyzing survey data from 4,684 mobile internet users from Hungary, Malaysia, Norway, Pakistan, Serbia, and Thailand. The cross-national analysis can highlight differences in trust among those countries, reveal potential cultural sources of trust, and support some generalization about trust in Facebook as a global phenomenon.

Trust in Facebook

Trust and its counterpart, vulnerability, may seem to be intuitive concepts, but scholars have long grappled with what exactly trust entails (e.g., Kee & Knox, 1970; Shapiro, 1987; Stern & Coleman, 2015). Myriad definitions of trust take divergent tacks but converge on a few key elements. There is a consensus that trust involves a trustor and trustee who are interdependent, a risky situation in which the trustor has entered voluntarily, and many conceptual layers (PytlikZillig & Kimbrough, 2016). An example of the conceptual layering is that the act of trusting contains a decision to trust, which contains an attitude about trust (Castelfranchi & Falcone, 2010, p. 37). The concept of trust may also refer to beliefs, attitudes, emotions, and predispositions, which reveal its multidimensional nature (Stern & Coleman, 2015).

One definition of trust involves a willingness by an individual "to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer, Davis, & Schoorman, 1995, p. 712). That willingness reflects a mental accounting of the costs and benefits of entering that vulnerable situation (Castelfranchi & Falcone, 2010), and scholars

have taken this view when theorizing about why people share personal information (Kehr, Kowatsch, Wentzel, & Fleisch, 2015). Commonly, these scholars draw on rational choice theories, which state that individuals act in a manner that maximizes utility or minimizes disutility when making choices among risky prospects (e.g., Luce, 1959; Schoemaker, 1982; Tversky & Kahneman, 1992). The rational component of trust suggests that it is a cognitive process based on judgment (Hardin, 2006); however, the phenomenon likely has both cognitive and affective components (Lewis & Weigert, 1985; McAllister, 1995). Indeed, emotion can help individuals make decisions in complex or unpredictable situations by prioritizing a subset of choices and aspects of information (Hanoch, 2002).

Many conceptualizations of trust are rooted in interpersonal research but have expanded to include trust in institutions. Some definitions of trust, like the one above, entail calculations of risk and vulnerability, where—in the case of interpersonal trust—individuals put themselves in the care of another and rely on that other not to take advantage of or harm them (Cole & Cohn, 2016). Other definitions refer to trust as confidence, which some researchers have reserved for describing institutions, and which trustors often develop from second-hand sources such as the mass media (Zmerli, Newton, & Montéro, 2007). Discussions of confidence appear primarily in research about political institutions, where trust depends on the belief that institutions meet normative expectations of responsiveness and responsibility (Miller & Listhaug, 1990).

Prior studies have looked at trust as a multidimensional concept. Beldad and Koehorst (2015) examined trust related to the technical competence to protect user privacy and the belief that other users will behave ethically. Beldad and Henger (2017) similarly defined trust in Facebook in terms of technical competence but also included trust relating to the ethical character of the social networking site. The distinction between competence and character has

appeared in other research (e.g., Malik, Hiekkanen, & Nieminen, 2016). Still, other conceptualizations regard the trustworthiness of the information appearing on Facebook (Escobar-Rodriguez, Gravalos-Gastaminza, & Perez-Calanas, 2017).

The current study focuses on character-based trust to conceptualize trust in Facebook. Specifically, trust in Facebook is the expectation individuals have that Facebook will not take advantage of them and, more generally, will not violate public expectations about how social networking sites should treat their users. This expectation may hinge on beliefs about how Facebook handles personal data, targets advertising, and respects the privacy of its users. Individuals will have low trust in Facebook if they believe that it is uncommitted to protecting or otherwise does not serve the interests of its users.

Trust in Data Institutions

For the purposes of this research, we describe Facebook as a type of data institution. Data institutions are entities that collect and analyze personal data to enhance their offerings. They can include technological institutions such as mobile service providers and social media companies, financial institutions such as banks and credit card companies, and government institutions, among others. Individuals are more likely to voluntarily share their personal data with these institutions when they have confidence their privacy will be protected (Beldad, van der Geest, de Jong, & Steehouder, 2012; Kehr et al., 2015; Taylor, Ferguson, & Ellen, 2015). Kehr et al. (2015) examined institutional trust in the context of smartphone apps, which they defined as "an individual's confidence that the data-requesting medium will not misuse his or her data" (p. 611). This confidence reflects a trust in data institutions.

Trust in data institutions is a kind of institutional trust. Scholars have approached the concept of institutional trust by considering where it originates. Mishler and Rose (2001)

described two competing perspectives. The first holds that institutional trust is a cultural phenomenon that exists outside personal experience, where individuals develop a sense of institutional trust early in life through socialization and learning a shared system of beliefs. This is called the *cultural argument*. The second perspective defines institutional trust as "the expected utility of institutions performing satisfactorily" (p. 31), where individuals base their expectations on what they have learned through their experience of institutions. This is called the *institutional argument*.

The distinction between cultural and experiential sources of institutional trust is important because it has implications for how individuals develop trust of distinct institutional entities. According to the cultural argument, individuals within the same cultural context should exhibit similar levels of trust of different kinds of institutions. Their trust of any one institution will reflect the broader culture of trust or distrust. Although prior research is more supportive of the institutional argument(e.g., Dahlberg & Linde, 2018; Seabo & Molefe, 2017), there may still be important cultural factors that underlie trust. One of these factors, for example, is uncertainty avoidance. According to Hofstede's model of culture, uncertainty avoidance reflects an intolerance of ambiguity, which manifests within cultures (Hofstede, 1984). This concept is relevant to trust because trust can resolve ambiguity. Such cultural factors within countries may lead to differences in trust between countries, which leads us to our first research question:

Research question 1 (RQ1): Does trust in Facebook differ between countries?

On the other hand, the institutional argument suggests that trust may vary among different kinds of institutions. This is because individuals evaluate institutions or types of institutions on a case-by-case basis. Thus, for example, when individuals compare different institutions, their perceptions of institutional quality can affect their levels of trust in those

institutions (Dahlberg & Linde, 2018). In keeping with that argument, when individuals have positive experiences sharing their data, they develop trust in data institutions. When they have negative experiences, they develop distrust. Subsequently, an experience-based institutional trust may be related to beliefs about specific institutional entities irrespective of cultural background.

Hypothesis 1 (H1): The greater the trust in data institutions, the higher the trust in Facebook.

This is an obvious prediction since we have argued that social networking companies, like Facebook, are a type of data institution. We include it in part to establishes a baseline explanatory model, which can clarify the relationship of trust with more interesting predictors. Our selection of predictors parallels the work of Park et al. (2012), who argued that reward-seeking compromise, affective concern, and cognitive knowledge influence consumers' willingness to provide personal data.

Model of Trust

Park et al. (2012) drew on affective and cognitive explanations of decision-making to explain privacy protection behaviors. The affective component reflects positive and negative feelings about a prospective behavior. They contrasted such feelings as fear, anxiety, and worry with feelings of trust, which can motivate privacy control. However, as we suggested earlier, the concept of trust is multifaceted, and it is restrictive to discuss it only in terms of affective states. The cognitive component reflects rational considerations about the prospective behavior. Park et al. (2012) defined this component mainly in terms of knowledge about privacy issues, arguing that individuals can more easily make decisions when they understand the context of the behavior. The affective-rational duality of human behavior is present in a number of theories, including many dual-process models (Bellini-Leite, 2018). Whereas affective routes to decision-

making tend to be fast and automatic, rational processes tend to be slow and more systematic (Kahneman, 2011). These routes can result in different outcomes. In addition, as Park et al. (2012) argued, cognitive appraisals of a privacy risk can amplify affective considerations when individuals make decisions about privacy control behaviors.

Complementing the affective and cognitive explanations of privacy-related behaviors, enticements by the trustee can help explain the apparent paradox between privacy concern and privacy control (Schumann, Wangenheim, & Groene, 2014). Individuals are more willing to share their personal information and relinquish privacy control when they expect to receive something for it in return, such as access to interesting content. Taken together, affective concern, cognitive knowledge, and reward-seeking compromise form a tripartite model explaining privacy control behaviors. Park et al. (2012) posed a research question concerning the three-way interaction of these factors. Their analysis showed that the relationship between concern and technical privacy control (e.g., clearing browser history) was slightly stronger for individuals with high privacy knowledge. For social privacy control (e.g., using a fake name online), this effect occurred only among those with high reward-seeking. We use the general structure of that tripartite model to explain trust in Facebook and begin with a discussion of reward-seeking compromise pertaining to consumers' acceptance of information personalization. Later, we review the concepts of privacy concern and privacy literacy to address the affective and cognitive elements of the model, respectively.

Acceptance of Information Personalization

The collection of personal data allows data institutions to customize the experience of the consumers they serve. Broadly this activity involves information personalization, as it affects the ways data institutions interact with consumers. For example, social media companies gather user

data in part to sell targeted advertising. Consequently, social media users see more advertising that is relevant to them, especially those who are members of niche consumer groups (Iyer, Soberman, & Villas-Boas, 2005; Johnson, 2013). This is useful for advertisers because individuals pay more attention to personalized advertisements, and more so when there are competing demands for their attention (Bang & Wojdynski, 2016).

Whereas information personalization benefits data institutions, it can be a mixed bag for consumers (Winter, 2014). Certainly, personalization benefits data institutions by helping them streamline their products and communicate more efficiently with their customers. In the case of advertising, personalization can benefit consumers by increasing competition among media content providers, resulting in lower costs to access content (Kox, Straathof, & Zwart, 2017). On the other hand, targeted advertising can result in consumers receiving more advertising and also, counterintuitively, advertising they prefer less (Johnson, 2013). Somewhat consistent with that observation, consumers are most accepting of targeted advertising not when they regard it as being personally relevant, but when they recognize the reciprocity of the arrangement: they share their data in exchange for a service they value (Schumann et al., 2014). Another example of this exchange is in online news consumption, where individuals are more accepting of personalized recommendations when they believe the recommendations will give them more diverse information (Bodó, Helberger, Eskens, & Möller, 2019).

Although there may be other factors that explain the acceptance of advertising targeting and, more broadly, information personalization, it follows that individuals are more accepting when they perceive a benefit. This process parallels the cognitive utility-based explanations of trust, where the perceived benefit of information personalization factors into the mental

accounting. The more that consumers accept their personal data as a currency for obtaining personalized services, the more they ought to trust the entities that provide those services.

Hypothesis 2 (H2): The greater the acceptance of information personalization, (a) the greater the trust in Facebook and (b) the greater the trust in data institutions.

General Privacy Concern

Affective utility-based explanations of choice can further clarify rational evaluative phenomena (Hanoch, 2002), such as trust. Individuals articulate their feelings about objects, ideas, and behaviors in the form of affective responses. Scholars have examined these responses in terms of positive and negative valence (Winkielman & Cacioppo, 2001) and with respect to specific emotions, such as happiness, sadness, and anger (Ainley, Hidi, & Berndorff, 2002). These responses can influence risk perceptions (Finucane, Alhakami, Slovic, & Johnson, 2000), which individuals consider when weighing the costs and benefits of entering a vulnerable situation. Case in point, individuals perceive lower risks of sensitive information disclosure when they experience positive affect (Kehr et al., 2015).

Another affect-related construct about the perceived risk of information disclosure is general privacy concern, which Kehr et al. (2015) conceptualized as a predisposition to worry about information privacy. This is a kind of negative affective response that arises when individuals see little benefit in sharing their private information and that a harmful breach of privacy is likely to occur (Youn, 2009). The harm in this instance has to do with negative outcomes, such as the loss of privacy, feelings of intrusion, identity theft, and potential embarrassment. Such conceptualization is consistent with a definition of privacy concerns as "beliefs about the risks and potential negative consequences associated with sharing information" (Baruh, Secinti, & Cemalcilar, 2017, p. 27).

If trust is an evaluative process of utility maximization, then privacy concern should result in lower levels of trust. Indeed, Bansal, Zahedi, and Gefen (2010) described privacy concern as a *disutility enhancer* because it reflects undesirable attributes of a choice decision that negatively impact its expected utility. This may be why individuals with privacy concern are more likely to engage in protective measures, such as deleting cookies and untagging photos, and less likely to share personal information (Baruh et al., 2017). Although the linkage between privacy concern and trust is intuitive, there are mixed empirical findings showing strong effects (Eastlick, Lotz, & Warrington, 2006), moderate effects (Malhotra, Kim, & Agarwal, 2004), weak effects (Chandra, 2009), and no effect (Bansal et al., 2010).

Privacy concern may point to a single entity, such as Facebook, or more broadly to a category of entities, such as online companies. The latter orientation is a predisposition to react negatively to the collection of personal data where there is the potential for a breach of privacy. This predisposition reflects beliefs about the nature of online personal data collection, storage, and use. It may also reflect beliefs about the motives of online companies in general. When companies collect more data than is necessary, users may be concerned about the reasons for the data collection. Such concern is negatively related to lower trust in online companies and should also be negatively related to trust in specific companies, like Facebook.

Hypothesis 3 (H3): The higher the general privacy concern, the lower the (a) trust in Facebook, (b) trust in data institutions, and (c) acceptance of information personalization.

Like our first prediction, this one is obvious and largely established in the extant literature. We include it in part as a replication of prior work and, more important, as a means of establishing its direct relationship with trust and acceptance of information personalization. We believe these linkages may depend on how well individuals understand privacy issues.

Privacy Literacy

For trustors, it is important to understand the intentions and future behaviors of trustees. This kind of understanding may reflect a knowledge of trustees that affects trustors' willingness to put themselves in vulnerable, trusting situations. Shapiro, Sheppard, and Cheraskin (1992) described this as knowledge-based trust, which they defined as the ability of trustors to predict the behaviors of trustees. This same kind of trust may arise in the context of Facebook, where users' understanding of Facebook's privacy policy may affect their beliefs about what the company does with user data and, subsequently, their use of Facebook. This is consistent with an early study of Facebook users, which found users self-reported more profile updating when they perceived they had not control over who could view their profile (Acquisti & Gross, 2006).

Knowledge about privacy reflects a kind of literacy, and researchers have described *privacy literacy* from many angles. Commonly, these conceptualizations refer to different kinds of knowledge. Park et al. (2013) split privacy literacy into a knowledge of the technical aspects of the internet, awareness of institutional practices, and understanding of privacy policies. Trepte et al. (2015) added knowledge about laws and regulations and knowledge of strategies to protect individual privacy. Those additional dimensions align with Park et al. (2012), who examined knowledge of regulatory protection and knowledge of data collection risk. They also align with Baruh et al. (2017), who distinguished between declarative knowledge about privacy risks and procedural knowledge about how to reduce personal exposure thereto. An equivalent idea appeared earlier in Langenderfer and Miyazaki (2009), who defined privacy literacy as "the understanding that consumers have of the information landscape with which they interact and their responsibilities within that landscape" (p. 383). Relevant to the current study, privacy

literacy includes an understanding of how data institutions collect and use personal data and how individuals can limit the unwanted use of those data.

Studies of privacy literacy have linked it with many other privacy-related constructs. Weinberger, Zhitomirsky-Geffet, and Bouhnik (2017) found that it was positively related to awareness of online surveillance, privacy concern, internet proficiency, and privacy self-efficacy. Ermakova, Baumann, Fabian, and Krasnova (2014) found that it was related to greater trust in Amazon, Twitter, and Yahoo, but not eBay or Facebook, after users read their privacy policies. In a meta-analysis, Baruh et al. (2017) found privacy literacy was positively related to intention to use online services (reliability-corrected correlation, $\rho = .38$), intention to use protective measures ($\rho = .15$), actual use of protective measures ($\rho = 36$), and privacy concern ($\rho = .14$). These findings suggest that privacy literacy is related to a constellation of individual cognitive and behavioral factors that would result in greater personal control over how data institutions can use personal data.

We are unaware of research linking privacy literacy with trust in Facebook, trust in data institutions, and acceptance of information tailoring. Further, we are uncertain of how it should be related to them. It is possible that individuals with high privacy literacy are more attuned to potential privacy breaches, which would be related to lower perceived utility of information personalization and lower trust. Alternatively, it may be that individuals with high privacy literacy feel more competent to protect their privacy and see less downside in trading personal data for information personalization. In that case, the relationships would be positive. In order to determine which, if either, explanation is correct, we ask the following research question:

Research question 2 (RQ2): What is the relationship between privacy literacy and (a) trust in Facebook, (b) trust in data institutions, and (c) acceptance of information personalization.

Finally, we are interested in understanding how privacy literacy may moderate the effects of privacy concern. Although most prior research has suggested a direct linkage between privacy literacy and privacy concern (Baruh et al., 2017; Weinberger et al., 2017), there is an argument that privacy literacy would moderate the effects of privacy concern. Specifically, the relationship of privacy concern with acceptance of information personalization and trust should be most pronounced among individuals with high privacy literacy. For those individuals, privacy concern may be especially diagnostic about the information and privacy risks they face and will be more influential in the formation of privacy-related beliefs. Park et al. (2012) found evidence, albeit a weak effect, in support of this argument, specifically that the relationship between privacy concern and privacy control was stronger among individuals with higher levels of privacy knowledge. Researchers have shown a similar effect in the context of health risk avoidance, where the association between health concern and medication adherence was significant only at moderate and high levels of health literacy (Shiyanbola, Unni, Huang, & Lanier, 2018). In other words, literacy facilitates individual action based on personal concern. We are unaware of research showing this moderation effect in the context of social media and trust, which the current study will examine.

Hypothesis 4 (H4): The greater the privacy literacy, the more negative the relationship between general privacy concern and (a) trust in Facebook, (b) trust in data institutions, and (c) acceptance of information personalization.

Method

Sample

A cross-sectional survey took place in July and August 2017 with sampling in Hungary, Malaysia, Norway, Pakistan, Serbia, and Thailand. These countries represent a range of human

development from medium (Pakistan) to very high (Norway), which affects access to communication technologies and internet use (United Nations Development Programme, 2018). In all but one country, the surveys were conducted using Kantar Lightspeed Web-panels with a qualifying condition that participants use the internet on their mobile phones. The exact details of remuneration are proprietary, but panel members receive points for participating in studies, which they may redeem for goods and services. In Pakistan, Kantar conducted computer-assisted telephone interviewing, but with the same qualifying condition regarding using mobile internet. Because quota sampling was used to ensure similar demographic profiles among the countries, the samples are not representative of the countries (see sample and census figures in Table 1). Except for Malaysia and Pakistan, the sampling overrepresents younger individuals. Except for Norway, the sampling overrepresents females. In total, there were 4,684 participants ranging in age from 18 to 55 (M = 27.50, SD = 5.04). The sample was 56% female and 44% male.

Measurement

We drew on prior operationalizations to measure trust in Facebook (Pavlou, 2003), privacy concern (Kobsa, Cho, & Knijnenburg, 2016; Pentina, Zhang, Bata, & Chen, 2016), and privacy literacy (Park & Mo Jang, 2014; Trepte et al., 2015). We developed measures of trust in data institutions and acceptance of information personalization using face-valid statements reflecting different data institutions and different methods of information personalization. We modeled these variables as latent constructs. Table 2 contains the wording, descriptive statistics, and factor loadings of the measurement items. In the next section, we evaluate the dimensionality of the measurement items and address our research questions and hypotheses using structural equation modeling.

Analysis

Measurement model. We used the default maximum likelihood estimator in Mplus 8.1 to conduct confirmatory factor analysis. This analysis treated all variables as continuous, including trust in data institutions as dichotomous-continuous. The model included unidirectional paths from latent factors to their indicators, bidirectional paths among latent factors, and one error correlation between two items measuring institutional trust (public administration and banks/financial institutions). We evaluated model fit using Hu and Bentler's (1999) joint information criteria of CFI > .95, RMSEA < .05 including the 90% confidence interval, and SRMR < .08. Based on the pooled sample, the model had good fit, χ^2 (178) = 1564.26, $p < .001$; CFI = .968; RMSEA = 0.041, 90% CI [0.039, 0.043]; SRMR = 0.040.

Next, we tested for measurement invariance between samples using reporting criteria from Putnick and Bornstein (2016). The model of configural invariance had good fit, χ^2 (1068) = 2471.05, $p < .001$; CFI = .963; RMSEA = 0.041, 90% CI [0.039, 0.043]; SRMR = 0.042. The model of metric invariance also had good fit, χ^2 (1148) = 2914.32, $p < .001$; CFI = .953; RMSEA = 0.044, 90% CI [0.042, 0.046]; SRMR = 0.056. Since the change in CFI was less than .02 and change in RMSEA and SRMR both less than .03, results supported an assumption of metric invariance. Finally, the model of scalar invariance had marginal fit, χ^2 (1228) = 4717.64, $p < .001$; CFI = .907; RMSEA = 0.060, 90% CI [0.059, 0.062]; SRMR = 0.074. Since the change in CFI was larger than .02 and change in SRMR larger than .015, the results did not support an assumption of scalar invariance. Since the answer to RQ1 requires scalar invariance on the measure of trust in Facebook, we estimated a one-factor model of trust in Facebook. However, the model of scalar invariance again had marginal fit, χ^2 (20) = 238.88, $p < .001$; CFI = .973;

RMSEA = 0.119, 90% CI [0.106, 0.133]; SRMR = 0.065. Also, change in both CFI and SRMR exceeded the thresholds.

Structural model. Because the structural model was saturated (see Figure 1), the fit statistics are identical to those from the CFA. We modeled the interaction of latent factors using a random effects model and the maximum likelihood estimator with robust standard errors using numerical integration. Because Mplus does not produce fit statistics for this analysis, we assessed model fit using the two-step method from Maslowsky, Jager, and Hemken (2015). This method first estimates a well-fitted model without the interaction term (i.e., the baseline model), producing the standard set of fit indices. Then, it estimates the model including the interaction term and conducts a log-likelihood ratio test, whose value (D) approximate a chi-square distribution. If that test is significant, then the model including the interaction term can also be considered well-fitted. For the pooled sample, the test was significant, $D(3) = 180.35$, $p < .001$. We extended this analysis to test for between-country differences in the structural model with metric invariance, which we draw on in the discussion. For each sub-sample, the log-likelihood ratio test was also significant. The appendix contains a table showing the log-likelihood ratio tests in addition to the baseline model fit statistics. Table 3 shows the unstandardized structural paths for the pooled and between-country analyses.

Results

As our CFA failed to show scalar invariance, it is not possible to answer RQ1. This is because we cannot be sure that differences in mean scores between countries show differences in trust. We examined the structural model for the pooled-sample model to test the hypotheses and answer RQ2. We examined the structural model for the pooled-sample model to test the hypotheses and answer the second research question.

First, results showed a positive relationship between trust in data institutions and trust in Facebook ($\beta = .29$, $p < .001$). Consistent with H1, this finding suggests that the greater the trust in a data institution, the greater the trust in Facebook.

Second, acceptance of information personalization was positively related to trust in Facebook ($\beta = .19$, $p < .001$). and trust in data institutions ($\beta = .18$, $p < .001$). Consistent with H2a and H2b, these findings suggest that the greater the acceptance of information personalization, the greater the trust in Facebook and in data institutions.

Third, privacy concern was negatively related to trust in Facebook ($\beta = -.03$, $p = .045$), trust in data institutions ($\beta = -.11$, $p < .001$), and acceptance of information personalization ($\beta = -.07$, $p < .001$). Although these effects are weak, they provide evidence in support H3a, H3b, and H3c, suggesting that individuals with greater privacy concern have lower trust in Facebook and data institutions, and are less accepting of information personalization.

Fourth, privacy literacy was negatively related to trust in Facebook ($\beta = -.36$, $p < .001$), trust in data institutions ($\beta = -.24$, $p < .001$), and acceptance of information personalization ($\beta = -.56$, $p < .001$). In answering RQ2, these findings suggest that individuals with greater the privacy literacy have lower trust in Facebook, and data institutions and are less accepting of information personalization.

Finally, privacy literacy significantly moderated the effect of privacy concern on trust in Facebook ($\beta = -.11$, $p < .001$), trust in data institutions ($\beta = -.06$, $p = .002$), and acceptance of information personalization ($\beta = -.17$, $p < .001$). These effects suggest that as privacy literacy increases, the effects of privacy concern on the dependent variables decrease. Figure 2 depicts these interactions, which are consistent with H4a, H4b, and H4c.

Discussion

This study considered cultural and experiential explanations of trust (Mishler & Rose, 2001) and evaluated a tripartite model of trust (Park et al., 2012). Analysis of cross-national data supported the hypothetical model explaining trust in Facebook, trust in data institutions, and acceptance of information personalization, and revealed differences between countries.

Cultural and Experiential Explanations of Trust

The results did not support a proper answer to the first research question, which had asked if trust in Facebook differs between countries. That question remains unanswered and it is likely that certain cultural factors matter for explaining trust. In the literature review, we had mentioned the cultural dimension of uncertainty avoidance, which refers to an intolerance of ambiguity, and may manifest as distrust. Intuitively, higher uncertainty avoidance would mean lower trust. It may also be that uncertainty avoidance, rather than predicting trust directly, moderates the effects of other trust antecedents. For example, Hwang and Lee (2012) found that social norms related to online shopping were more strongly related to trust in online shopping among individuals with high uncertainty avoidance. Focusing on culture-related factors at the individual level, rather than the country level might prove more fruitful in studies explaining trust. Though, culture may ultimately have limited import in this kind of research. As Dinesen (2011) wrote, “while trust may to some extent be culturally inherited and sticky, it is still subject to change under certain conditions” (p. 115).

In contrast with the cultural explanation, the experiential explanation of trust suggests that people form trusting beliefs based on their prior experiences with trust-bearing institutions. Drawing on that perspective, we argued that trust in Facebook reflects broader beliefs about data institutions, which individuals may develop across multiple interactions. In support of our

prediction, we found that trust in Facebook is positively related to trust in data institutions. It should be noted that only certain kinds of data companies depend on user data for targeted advertising, and the concept of a data institution goes beyond any specific uses of user data. This underscores the fact that trust in data institutions is a general sentiment rather than being company-specific. This characterization can help explain why trust in data institutions did not strongly predict trust in Facebook, despite that relationship being rather obvious. Indeed, the CFA results showed the two variables were moderately correlated (r = .52), suggesting they are related but distinct constructs. Also embedded in this point is the fact that no two data institutions are alike. Whereas some institutions prioritize data protection, others might prioritize the monetization of data (see Turow & Hennessy, 2007, p. 315). The main benefit of modeling this relationship, at least for the purposes of this study, was that it controlled for some of the trust Facebook has in common with other data institutions. This facilitated analyzing trust-related factors more specific to Facebook, which we discuss below.

Tripartite Model of Trust

We introduced the tripartite model of trust to explain trust in relation to acceptance of information personalization, general privacy concern, and privacy literacy. Although some of the observed relationships were weak, we had consistent support for our hypotheses. These findings have theoretical implications regarding the tripartite model that Park et al. (2012) used to explain privacy protection. Given the current findings, it would be theoretically interesting to know if trust mediates the relationship between the antecedent variables and privacy-related behaviors. That could be the task of a future study. These findings also have practical implications for data institutions, which we discuss below.

As predicted, user acceptance of information personalization was related to trust in Facebook and data institutions. The current study did not try to tease out causality, but there are reasonable arguments for both causal directions. On the one hand, trust involves mental accounting of the benefits users stand to gain in exchange for sharing personal information (Castelfranchi & Falcone, 2010). Users who regard information personalization as a benefit may have greater trust because of a perceived reciprocity in their dealings with data institutions (Schumann et al., 2014). This is especially important because information personalization can make users feel more vulnerable about their data sharing (Aguirre, Mahr, de Ruyters, & Wetzels, 2015). This argument is consistent with the rationale of Park et al. (2012). Yet, it is also plausible that the causal ordering is reversed, where acceptance of personalization stems from trust. Users are unlikely to see a benefit in personalized information if they do not trust the source. This means that trust is and will continue to be an important factor in the business of Facebook and other data-driven companies. To the extent that personalization, which can be so many things, is a competitive advantage, less trusted companies will struggle to extract value from it (see also, Kalaignanam, Kushwaha, & Rajavi, 2018).

Underscoring the importance of vulnerability, we found that general privacy concern—which reflects a state of perceived vulnerability (Baruh et al., 2017)—is negatively related to trust and acceptance of information personalization. These linkages constitute the affective portion of the tripartite model, suggesting that privacy-related attitudes and beliefs are related to emotion, albeit weakly. Dual process models suggest that emotion has heuristic value and can lead to more automatic and intuitive decision-making (Kahneman, 2011). Not only does this mean that Facebook and similar companies may suffer when there are global privacy scandals, but also that rational appeals about new privacy measures may be ineffective if they do not

address underlying negative affect. Then again, given the weak main effects of privacy concern, these assertions have limited practical implications.

The implications of privacy concern become clearer when accounting for privacy literacy, which pertains to the more cognitive portion of the tripartite model. First, we found that privacy literacy is negatively related to trust and acceptance of information personalization. The utility-basis of trust implies some reasoning about prospective costs and benefits. Individuals with high privacy literacy better understand the limitations of privacy protections, and the costs of privacy risks are more pronounced in their mental accounting of trust. Consistent with this argument, privacy literacy was most negatively related to acceptance of information personalization. Among privacy-literate individuals, the perceived costs of sharing personal data outweigh the expected benefits of personalization. This finding is somewhat counter to the point that Turow and Hennessy (2007) made about *privacy paralysis*, which they used to explain the privacy paradox. They suggested that individuals share personal data despite privacy concerns because they are confused about whether data institutions will protect or disclose their personal data. Such paralysis is likely a real occurrence, but it is also the case that privacy literacy can directly reduce confusion and lead to concrete and actionable trust-related beliefs. As the current results showed, privacy literacy was negatively related to trust. Individuals who understand how data institutions collect and use personal data will tend to be less trusting of them. Although this study did not test for indirect effects, it may be that this distrust stems from a rejection of information personalization.

Second, we found that the greater the privacy literacy the stronger the relationship of privacy concern with trust and acceptance of information personalization. Although the effects were small, especially on trust in data institutions, they show the interplay of thoughts and

feelings in forming trusting beliefs. As we argued previously, privacy concern is more diagnostic of potential privacy risks when individuals have high privacy literacy. These individuals can probably identify the causes of their concern, and their concern becomes specifically useful in their mental accounting of trust. In other words, they reason about their emotion, integrating it into a more systematic assessment of trust. Prior research has found a similar effect in the context of health behavior, showing the importance of health literacy in medication adherence (Shiyanbola et al., 2018). Likewise, the current findings show the importance of privacy literacy in relation to trust, which may ultimately impact privacy-related behaviors. These findings underscore the importance of privacy literacy education which formal instruction and public service campaigns can support (Wissinger, 2017).

Limitations and Directions for Future Research

This study has three limitations with respect to the sample. First, as the data are cross-sectional, the analysis cannot show temporality, and thus cannot support causal claims. Experimentation would strengthen current findings—for example, to clarify the relationship between acceptance of information personalization and trust—by allowing tests of causation. Second, online survey panel members do not necessarily represent the general public. Although online panels may be acceptable for experimentation (Mullinix, Leeper, Druckman, & Freese, 2015), they may have demographic and psychographic idiosyncrasies that would limit the generalizability of survey research. Relevant to the current study, one study compared six major survey panels and found differences among them with respect to privacy comfort (Schnorf, Sedley, Ortlieb, & Woodruff, 2014). Further, it is intuitive that panel members—who willingly share their opinions with a survey company—have a distinct view on privacy. Third, the large

sample size means that practically insignificant results may be statistically significant. Because of this, we included the effect sizes in Table 3 so that readers may draw their own conclusions.

Another limitation is more conceptual. One of the reasons to study concepts like trust is to better understand the privacy paradox, or the observation that individuals share personal information despite being concerned about their privacy (Norberg, Horne, & Horne, 2007). The current study sought to understand the issue of trust by looking at individual differences on psychological concepts. This emphasis ignored a more sociological perspective, which could add important layers to the trust issue. One thing that may explain why people continue to use Facebook even though they realize that it is not trustworthy is that it is structured into their everyday interactions. Thus, they may have concern that their information will be stolen or lives surveilled, but since it has become integral to their social interactions, they are willing to accept this vulnerability. This is, in a sense, the price they are willing to pay for access to the platform and is an explanation of the privacy paradox that parallels the mental accounting perspective (Kokolakis, 2017). Future research can expand on the current explanation of trust by accounting for the social value of data-driven companies like Facebook.

Conclusion

Trust is important for Facebook and other companies using consumer data as part of their business. This trust varies among individuals, perhaps as an intrinsic sentiment, and is correlated with privacy concern and privacy literacy. It reflects a mental accounting of risks and benefits, including the perceived benefits of information personalization. We believe that the increased use of data is likely to change as consumers generate more data and companies develop new methods of using those data and providing services to consumers in exchange. Our findings show that increases in privacy concern and literacy are coincident with a decrease in trust, but

that trust increases when consumers see value in information personalization. These factors of affect, cognition, and reward-seeking compromise comprise a tripartite model of trust, and companies that hope to gain the trust of consumers need to address all three components.

Table 1

Distributions of demographics and model variables by country

	Sample				Census	
Country	*N*	Age Range	Age *M* (*SD*)	% Female	Age	% Female
1. Hungary	755	18-38	27.66 (5.08)	55	42.7	52
2. Malaysia	852	18-50	27.94 (5.03)	60	28.7	46
3. Norway	801	18-35	27.27 (4.52)	45	39.3	47
4. Pakistan	719	18-35	26.68 (5.41)	51	24.1	45
5. Serbia	718	18-55	27.42 (4.97)	68	42.8	50
6. Thailand	839	18-43	27.92 (5.13)	56	38.1	49

Note. Census figures are from the CIA World Fact Book.

Table 2

Summary of measurement

Variable/item	*M*	*SD*	*λ*
Trust in Facebook			
Facebook is trustworthy.	2.88	1.04	.88
Facebook keeps promises and commitments.	2.98	0.98	.86
I trust Facebook because they keep my best interests in mind.	2.85	1.05	.90
Trust in Data Institutions			
Handset suppliers	0.43	0.45	.74
Mobile operators	0.52	0.46	.75
Social media players	0.31	0.42	.64
Public administration e.g. tax authority	0.60	0.45	.46
Banks/financial institutions	0.62	0.45	.55
Acceptance of Information Personalization			
Apps and Internet services tailored to your preferences and needs	3.22	1.07	.87
Customer service tailored to your preferences and needs	3.26	1.04	.85
Advertisements tailored to your preferences and needs	3.01	1.16	.83
General Privacy Concern			
It usually bothers me when mobile applications ask me for personal information.	3.89	0.90	.74
It bothers me that personal information given to online companies for a specific purpose can be used for other purposes.	4.02	0.89	.75
I am concerned that online companies are collecting too much personal information about me	3.87	0.93	.74
I believe that mobile applications ask for more data than what is needed to fulfill the purpose of the app	3.86	0.92	.62
It bothers me when I cannot control how my personal information is used by online companies	3.97	0.90	.75
Privacy literacy (all items reverse-coded)			
When a mobile app has a privacy policy it means that no personal data is shared with other apps or companies.	2.65	1.11	.63
Facebook, Google and similar companies delete personal data after a pre-defined period.	3.00	1.11	.64
App providers only collect personal information that is needed to deliver the service.	2.86	1.15	.75
When you deactivate GPS on your phone, your location cannot be tracked.	2.93	1.24	.62
It is not possible to hack into private information on a mobile phone.	3.47	1.33	.68

Note. Trust in Facebook, general privacy concern, and privacy literacy used Likert scaling ranging from 1 (*strongly disagree*) to 5 (*strongly agree*). Trust in data institutions had the stem, "Do you trust that these actors don't misuse the data you leave when you register and use their services and apps?" Response options were 0 (*no*) and 1 (*yes*). Acceptance of information personalization had the stem, "In general, would you approve use of your personal data if the purpose is to offer you any of the following benefits?" Response options ranged from 1 (*very unlikely*) to 5 (*very likely*). λ is the standardized factor loading from confirmatory factor analysis using the pooled sample.

Table 3

Unstandardized structural model paths for the pooled sample and each country

Variables		Pooled Sample			Hungary			Malaysia			Norway			Pakistan			Serbia			Thailand		
		B	*SE*	*p*	*B*	*SE*	*p*	*B*	*SE*	*p*	*B*	*SE*	*p*	*B*	*SE*	*p*	*B*	*SE*	*p*	*B*	*SE*	*p*
TF ←	TDI	0.74	0.05	<.001	0.65^{a,b}	0.10	<.001	0.65^{a,b}	0.09	<.001	1.59	0.16	<.001	0.88^{a}	0.13	<.001	0.60^{a,b}	0.13	<.001	0.48^{b}	0.11	<.001
	AIP	0.21	0.02	<.001	0.22^{a}	0.05	<.001	0.13^{a,b}	0.06	.041	0.06^{b}	0.05	.199	0.23^{a}	0.06	<.001	0.15^{a,b}	0.05	.004	0.27^{a}	0.06	<.001
	GPC	-0.04	0.02	.045	-0.10^{a,b}	0.05	.068	0.02^{a}	0.05	.695	0.01^{a,b,c}	0.07	.891	0.20^{c}	0.07	.006	-0.15^{b}	0.05	.007	-0.05^{a,b}	0.04	.210
	PL	-0.47	0.03	<.001	-0.35^{a,b}	0.05	<.001	-0.34^{a,b}	0.08	<.001	-0.49^{a}	0.09	<.001	-0.20^{b}	0.11	.060	-0.41^{a,b}	0.09	<.001	-0.31^{a,b}	0.06	<.001
	INT	-0.21	0.04	<.001	-0.03^{a,b}	0.07	.679	-0.47^{c}	0.11	<.001	0.16^{a}	0.11	.144	-0.41^{c}	0.15	.006	-0.22^{b,c}	0.09	.015	-0.27^{c}	0.06	<.001
R^2		.51			.45			.42			.62			.30			.39			.50		
TDI ←	AIP	0.08	0.01	<.001	0.10^{a}	0.02	<.001	0.19^{b}	0.03	<.001	0.03^{c}	0.02	.239	0.11^{a}	0.03	<.001	0.09^{a,c}	0.03	<.001	0.15^{a,b}	0.03	<.001
	GPC	-0.06	0.01	<.001	-0.06^{a}	0.03	.015	-0.10^{a,b}	0.03	<.001	-0.15^{b}	0.03	<.001	-0.03^{a}	0.03	.294	-0.05^{a}	0.03	.083	-0.05^{a}	0.03	.039
	PL	-0.12	0.01	<.001	-0.14^{a}	0.02	<.001	-0.14^{a,b}	0.04	.002	-0.13^{a,b}	0.04	<.001	-0.15^{a,b}	0.05	<.001	-0.19^{a,b}	0.04	<.001	-0.23^{b}	0.03	<.001
	INT	-0.05	0.02	.002	0.02^{a,b}	0.02	.450	0.07^{a}	0.05	.141	-0.20^{c}	0.06	<.001	-0.06^{a,b,c}	0.06	.307	0.05^{a}	0.04	.157	-0.07^{b}	0.04	.065
R^2		.19			.23			.25			.33			.14			.25			.38		
AIP ←	GPC	-0.09	0.02	<.001	-0.16^{a,b}	0.06	.006	0.10^{c}	0.05	.027	-0.38^{d}	0.06	<.001	-0.07^{a}	0.05	.205	-0.28^{b,d}	0.05	<.001	0.22^{c}	0.04	<.001
	PL	-0.67	0.03	<.001	-0.37^{a}	0.05	<.001	-0.57^{b}	0.06	<.001	-0.54^{a,b}	0.09	<.001	-0.68^{b}	0.09	<.001	-0.60^{b}	0.08	<.001	-0.51^{a,b}	0.05	<.001
	INT	-0.31	0.04	<.001	-0.32^{a}	0.07	<.001	-0.35^{a}	0.12	.005	-0.12^{a,b}	0.10	.235	0.02^{b}	0.13	.890	-0.15^{a,b}	0.10	.106	-0.16^{a,b}	0.08	.039
R^2		.40			.25			.30			.31			.19			.31			.33		
GPC ↔	PL	0.10	0.01	<.001	0.16^{a}	0.03	<.001	0.07	0.02	<.001	0.17^{a}	0.02	<.001	-0.09^{b}	0.02	<.001	0.13^{a}	0.02	<.001	-0.06^{b}	0.02	<.001

Note. TF = trust in Facebook. TDI = trust in data institutions. AIP = acceptance of information personalization. GPC = general privacy concerns. PL = privacy literacy. INT = interaction of general privacy concerns and privacy literacy. The models estimated for each country sub-sample had metric invariance where the factor structure was constrained to be equal and paths among latent factors were estimated freely. For comparisons among countries (across rows), parameter estimates sharing the same superscript are not significantly different (calculated *z*-score, $p < .05$). The calculation of *z*-scores used the method described by Paternoster, Brame, Mazerolle, and Piquero (1998).

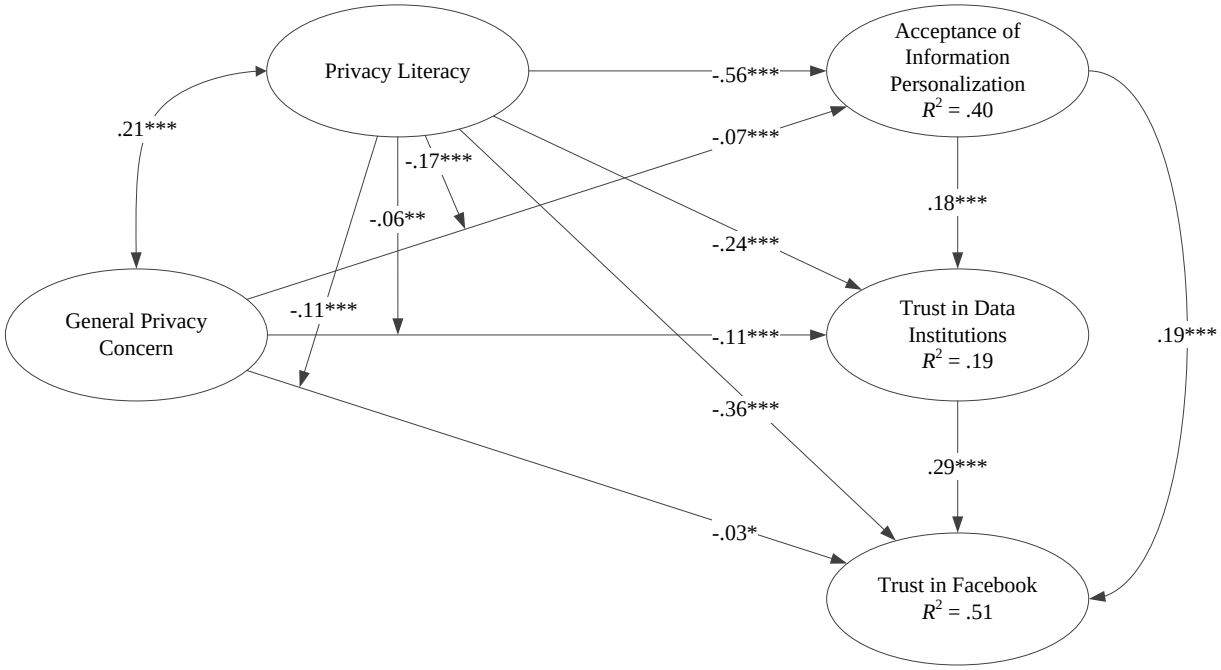

Figure 1. Structural model with standardized estimates based on the pooled sample

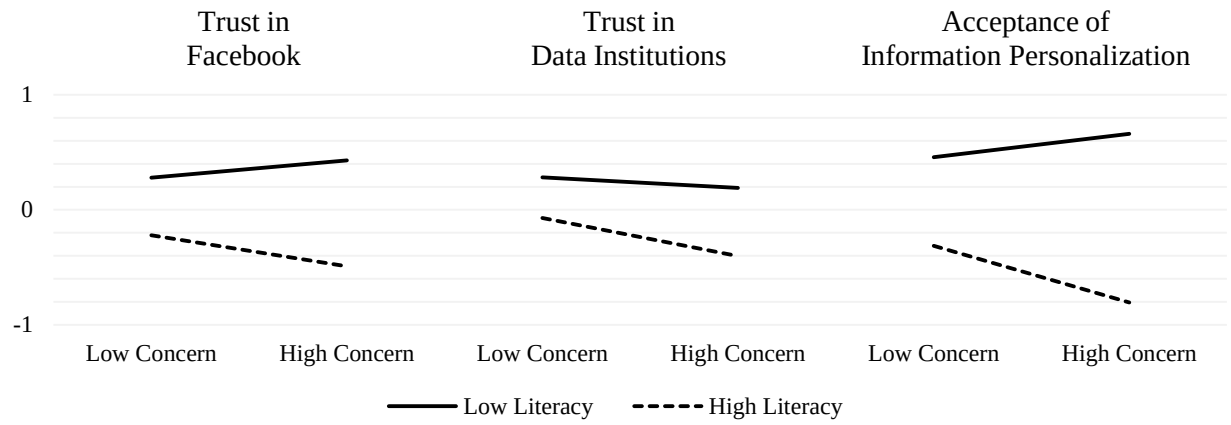

Figure 2. The standardized interaction effects of general privacy concern and privacy literacy in the prediction of trust in Facebook, trust in data institutions, and acceptance of information personalization based on the pooled sample. The vertical axis shows $M \pm 1SD$ values of the dependent variables. The high and low values of the independent variables reflect $M \pm 1SD$.

Appendix

Table

Fit statistics and log-likelihood ratio tests for CFA and SEM

Model	Fit statistics for CFA/SEM					Log-likelihood ratio tests					
	χ^2	*df*	CFI	RMSEA [90% CI]	SRMR	LL_0	df_0	LL_1	df_1	$D(3)$	*p*
Configural invariance	2403.78	1062	.964	.040 [.038, .042]	.041						
Metric invariance	2833.88	1142	.955	.044 [.042, .046]	.055						
Scalar invariance	4484.91	1222	.913	.058 [.057, .060]	.073						
Pooled sample	1390.09	177	.972	.038 [.036, .040]	.039	-101013.48	75	-100923.31	78	180.35	<.001
Hungary	415.94	193	.966	.039 [.034, .044]	.046	-16942.01	59	-16927.71	62	28.61	<.001
Malaysia	426.86	193	.961	.038 [.033, .043]	.058	-17257.12	59	-17234.87	62	44.50	<.001
Norway	743.14	193	.912	.060 [.055, .064]	.075	-16931.01	59	-16919.61	62	22.81	<.001
Pakistan	369.66	193	.969	.036 [.030, .041]	.048	-15711.37	59	-15703.21	62	16.31	<.001
Serbia	405.34	193	.966	.039 [.034, .044]	.046	-14537.00	59	-14531.94	62	10.13	0.008
Thailand	472.95	193	.959	.042 [.037, .046]	.052	-16480.54	59	-16466.06	62	28.96	<.001

Note. The models estimated for each country sub-sample had metric invariance where the factor structure was constrained to be equal and paths among latent factors were estimated freely. The sub-scripts, 0 and 1, denote the log-likelihood ratios and degrees of freedom for the baseline model (0) and interaction model (1).

References

Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on the Facebook*, Berlin, Heidelberg.

Aguirre, E., Mahr, D., de Ruyters, J. C., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing, 91*(1), 34-49. doi:10.1016/j.jretai.2014.09.005

Ainley, M., Hidi, S., & Berndorff, D. (2002). Interest, learning, and the psychological processes that mediate their relationship. *Journal of Educational Psychology, 94*(3), 545-561. doi:10.1037//0022-0663.94.3.545

Badshah, N. (2018, 8 April). Facebook to contact 87 million users affected by data breach. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach

Bang, H., & Wojdynski, B. W. (2016). Tracking users' visual attention and responses to personalized advertising based on task cognitive demand. *Computers in Human Behavior, 55*, 867-876. doi:10.1016/j.chb.2015.10.025

Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138-150. doi:10.1016/j.dss.2010.01.010

Barrett, B. (2018, 12 October). How to check if your Facebook account got hacked—and how badly. *Wired*. Retrieved from https://www.wired.com/story/facebook-hack-check-if-account-affected/

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

Beldad, A. D., & Hegner, S. M. (2017). More photos from me to thee: Factors influencing the intention to continue sharing personal photos on an online social networking (OSN) site among young adults in the Netherlands. *International Journal of Human–Computer Interaction, 33*(5), 410-422. doi:10.1080/10447318.2016.1254890

Beldad, A. D., & Koehorst, R. (2015). It's not about the risks, I'm just used to doing it: Disclosure of personal information on Facebook among adolescent Dutch users. In G. Meiselwitz (Ed.), *Social Computing and Social Media, SCSM 2015* (Vol. 9182, pp. 185-195). Berlin: Springer-Verlag Berlin.

Beldad, A. D., van der Geest, T., de Jong, M., & Steehouder, M. (2012). Shall I tell you where i live and who I am? Factors influencing the behavioral intention to disclose personal data for online government transactions. *International Journal of Human–Computer Interaction, 28*(3), 163-177. doi:10.1080/10447318.2011.572331

Bellini-Leite, S. C. (2018). Dual process theory: Systems, types, minds, modes, kinds or metaphors? A critical review. *Review of Philosophy and Psychology, 9*(2), 213-225. doi:10.1007/s13164-017-0376-x

Bodó, B., Helberger, N., Eskens, S., & Möller, J. (2019). Interested in diversity. *Digital Journalism, 7*(2), 206-229. doi:10.1080/21670811.2018.1521292

Castelfranchi, C., & Falcone, R. (2010). *Trust theory : A socio-cognitive and computational model*. New York: Wiley.

Chandra, A. (2009). Targeted advertising: The role of subscriber characteristics in media markets. *Journal of Industrial Economics, 57*(1), 58-84. doi:10.1111/j.1467-6451.2009.00370.x

Cole, L. M., & Cohn, E. S. (2016). Institutional trust across cultures: its definitions, conceptualizations, and antecedents across Eastern and Western European nations. In E. Shockley, T. M. S. Neal, & B. H. Bornstein (Eds.), *Interdisciplinary perspectives on trust: Towards theoretical and methodological integration* (pp. 157-176): Springer International Publishing.

Dahlberg, S., & Linde, J. (2018). Socialization or experience? Institutional trust and satisfaction with democracy among emigrants in different institutional settings. *The Journal of Politics, 0*(0), 1389-1393. doi:10.1086/698661

Dinesen, P. T. (2011). Where you come from or where you live? Examining the cultural and institutional explanation of generalized trust using migration as a natural experiment. *European Sociological Review, 29*(1), 114-128. doi:10.1093/esr/jcr044

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research, 59*(8), 877-886. doi:10.1016/j.jbusres.2006.02.006

Ermakova, T., Baumann, A., Fabian, B., & Krasnova, H. (2014). *Privacy policies and users' trust: Does readability matter?* Paper presented at the Americas Conference on Information Systems, Savannah, GA.

Escobar-Rodriguez, T., Gravalos-Gastaminza, M. A., & Perez-Calanas, C. (2017). Facebook and the intention of purchasing tourism products: Moderating effects of gender, age and marital status. *Scandinavian Journal of Hospitality and Tourism, 17*(2), 129-144. doi:10.1080/15022250.2015.1137784

Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M. (2000). The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making, 13*(1), 1-17. doi:10.1002/(sici)1099-0771(200001/03)13:1<1::Aid-bdm333>3.0.Co;2-s

Hanoch, Y. (2002). "Neither an angel nor an ant": Emotion as an aid to bounded rationality. *Journal of Economic Psychology, 23*(1), 1-25. doi:10.1016/S0167-4870(01)00065-4

Hardin, R. (2006). *Trust*. Malden, MA: Polity.

Hofstede, G. (1984). *Culture's consequences: International differences in work-related values (abridged edition)*. Newbury Park, CA: Sage.

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

Hwang, Y., & Lee, K. C. (2012). Investigating the moderating role of uncertainty avoidance cultural values on multidimensional online trust. *Information & Management, 49*(3), 171-176. doi:10.1016/j.im.2012.02.003

Iyer, G., Soberman, D., & Villas-Boas, J. M. (2005). The targeting of advertising. *Marketing Science, 24*(3), 461-476. doi:10.1287/mksc.1050.0117

Johnson, J. P. (2013). Targeted advertising and advertising avoidance. *The RAND Journal of Economics, 44*(1), 128-144. doi:10.1111/1756-2171.12014

Kahneman, D. (2011). *Thinking, fast and slow*. New York: Farrar, Strauss, Giroux.

Kalaignanam, K., Kushwaha, T., & Rajavi, K. (2018). How does web personalization create value for online retailers? Lower cash flow volatility or enhanced cash flows. *Journal of Retailing, 94*(3), 265-279. doi:10.1016/j.jretai.2018.05.001

Kee, H. W., & Knox, R. E. (1970). Conceptual and methodological considerations in the study of trust and suspicion. *The Journal of Conflict Resolution, 14*(3), 357-366. doi:10.2307/173516

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607-635. doi:10.1111/isj.12062

Kobsa, A., Cho, H., & Knijnenburg, B. P. (2016). The effect of personalization provider characteristics on privacy attitudes and behaviors: An Elaboration Likelihood Model approach. *Journal of the Association for Information Science and Technology, 67*(11), 2587-2606. doi:10.1002/asi.23629

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

Kox, H., Straathof, B., & Zwart, G. (2017). Targeted advertising, platform competition, and privacy. *Journal of Economics & Management Strategy, 26*(3), 557-570. doi:10.1111/jems.12200

Langenderfer, J., & Miyazaki, A. D. (2009). Privacy in the Information Economy. *Journal of Consumer Affairs, 43*(3), 380-388. doi:10.1111/j.1745-6606.2009.01152.x

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social Forces, 63*(4), 967-985. doi:10.2307/2578601

Luce, R. D. (1959). *Individual choice behavior: A theoretical analysis*. New York: Wiley.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355. doi:10.1287/isre.1040.0032

Malik, A., Hiekkanen, K., & Nieminen, M. (2016). Privacy and trust in Facebook photo sharing: Age and gender differences. *Program-Electronic Library and Information Systems, 50*(4), 462-480. doi:10.1108/prog-02-2016-0012

Maslowsky, J., Jager, J., & Hemken, D. (2015). Estimating and interpreting latent variable interactions: A tutorial for applying the latent moderated structural equations method. *International journal of behavioral development, 39*(1), 87-96. doi:10.1177/0165025414552301

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review, 20*(3), 709-734. doi:10.2307/258792

McAllister, D. J. (1995). Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal, 38*(1), 24-59. doi:10.5465/256727

Miller, A. H., & Listhaug, O. (1990). Political parties and confidence in government: A comparison of Norway, Sweden and the United States. *British Journal of Political Science, 20*(3), 357-386. doi:10.1017/S0007123400005883

Mishler, W., & Rose, R. (2001). *What are the origins of political trust? Testing institutional and cultural theories in post-communist societies* (Vol. 34).

Mullinix, K. J., Leeper, T. J., Druckman, J. N., & Freese, J. (2015). The generalizability of survey experiments. *Journal of Experimental Political Science, 2*(2), 109-138. doi:10.1017/XPS.2015.19

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. doi:10.1111/j.1745-6606.2006.00070.x

O'Flaherty, K. (2018, 10 October). This is why people no longer trust Google and Facebook with their data. *Forbes*. Retrieved from https://www.forbes.com/sites/kateoflahertyuk/2018/10/10/this-is-why-people-no-longer-trust-google-and-facebook-with-their-data

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215-236. doi:10.1177/0093650211418338

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. doi:10.1016/j.chb.2012.01.004

Park, Y. J., & Mo Jang, S. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior, 38*, 296-303. doi:10.1016/j.chb.2014.05.041

Paternoster, R., Brame, R., Mazerolle, P., & Piquero, A. (1998). Using the correct statistical test for the equality of regression coefficients. *Criminology, 36*(4), 859-866. doi:10.1111/j.1745-9125.1998.tb01268.x

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101-134.

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior, 65*, 409-419. doi:10.1016/j.chb.2016.09.005

Putnick, D. L., & Bornstein, M. H. (2016). Measurement invariance conventions and reporting: The state of the art and future directions for psychological research. *Developmental review : DR, 41*, 71-90. doi:10.1016/j.dr.2016.06.004

PytlikZillig, L. M., & Kimbrough, C. D. (2016). Consensus on conceptualizations and definitions of trust: Are we there yet? In E. Shockley, T. M. S. Neal, & B. H. Bornstein (Eds.), *Interdisciplinary perspectives on trust: Towards theoretical and methodological integration* (pp. 17-47): Springer International Publishing.

Schnorf, S., Sedley, A., Ortlieb, M., & Woodruff, A. (2014). *A comparison of six sample providers regarding online privacy benchmarks*. Paper presented at the SOUPS Workshop on Privacy Personas and Segmentation, Menlo Park, CA.

Schoemaker, P. J. H. (1982). The expected utility model: Its variants, purposes, evidence and limitations. *Journal of Economic Literature, 20*(2), 529-563.

Schumann, J. H., Wangenheim, F. v., & Groene, N. (2014). Targeted online advertising: Using reciprocity appeals to increase acceptance among users of free web services. *Journal of Marketing, 78*(1), 59-75. doi:10.1509/jm.11.0316

Seabo, B., & Molefe, W. (2017). The determinants of institutional trust in Botswana's liberal democracy. *African Journal of Political Science and International Relations, 11*(3), 36-49. doi:10.5897/AJPSIR2016.0943

Shapiro, D. L., Sheppard, B. H., & Cheraskin, L. (1992). Business on a handshake. *Negotiation Journal, 8*(4), 365-377. doi:10.1111/j.1571-9979.1992.tb00679.x

Shapiro, S. P. (1987). The social control of impersonal trust. *American Journal of Sociology, 93*(3), 623-658.

Shiyanbola, O. O., Unni, E., Huang, Y.-M., & Lanier, C. (2018). The association of health literacy with illness perceptions, medication beliefs, and medication adherence among individuals with type 2 diabetes. *Research in Social and Administrative Pharmacy, 14*(9), 824-830. doi:10.1016/j.sapharm.2017.12.005

Stern, M. J., & Coleman, K. J. (2015). The multidimensionality of trust: Applications in collaborative natural resource management. *Society & Natural Resources, 28*(2), 117-132. doi:10.1080/08941920.2014.945062

Taylor, J. F., Ferguson, J., & Ellen, P. S. (2015). From trait to state: understanding privacy concerns. *Journal of Consumer Marketing, 32*(2), 99-112. doi:10.1108/jcm-07-2014-1078

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European Data Protection Law* (pp. 333-365). Dordrecht: Springer Netherlands.

Turow, J., & Hennessy, M. (2007). Internet privacy and institutional trust: Insights from a national survey. *New Media & Society, 9*(2), 300-318. doi:10.1177/1461444807072219

Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty, 5*(4), 297-323. doi:10.1007/BF00122574

United Nations Development Programme. (2018). *Human development indices and indicators*. New York: United Nations Development Programme Retrieved from http://hdr.undp.org/sites/default/files/2018_human_development_statistical_update.pdf.

Weinberger, M., Zhitomirsky-Geffet, M., & Bouhnik, D. (2017). Factors affecting users' online privacy literacy among students in Israel. *Online Information Review, 41*(5), 655-671. doi:10.1108/oir-05-2016-0127

Winkielman, P., & Cacioppo, J. T. (2001). Mind at ease puts a smile on the face: Psychophysiological evidence that processing facilitation elicits positive affect. *Journal of Personality and Social Psychology, 81*(6), 989-1000. doi:10.1037//0022-3514.81.6.989

Winter, J. S. (2014). Surveillance in ubiquitous network societies: Normative conflicts related to the consumer in-store supermarket experience in the context of the Internet of Things. *Ethics and Information Technology, 16*(1), 27-41. doi:10.1007/s10676-013-9332-3

Wissinger, C. L. (2017). Privacy literacy: From theory to practice. *Communications in Information Literacy, 11*(2), 378-389. doi:10.15760/comminfolit.2017.11.2.9

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389-418. doi:10.1111/j.1745-6606.2009.01146.x

Zmerli, S., Newton, K., & Montéro, J. R. (2007). Trust in people, confidence in political institutions, and satisfaction with democracy. In J. W. van Deth, J. R. Montero, & A. Westholm (Eds.), *Citizenship and involvement in European democracies. A comparative analysis* (pp. 35-65). London: Routledge.