WhatsApp marketing: A study on WhatsApp brand communication and the role of trust in self-disclosure

Zarouali, B.; Brosius, A.; Helberger, N.; de Vreese, C.H.

Publication date
2021

Document Version
Final published version

Published in
International Journal of Communication

International Journal of Communication 15(2021), 252–276 1932–8036/20210005

WhatsApp Marketing: A Study on WhatsApp Brand Communication and the Role of Trust in Self-Disclosure

BRAHIM ZAROUALI
ANNA BROSIUS
NATALI HELBERGER
CLAES H. DE VREESE
University of Amsterdam, The Netherlands

Recently, WhatsApp allowed commercial brands to initiate private chat conversations with users through their direct messaging platform. With more than 1 billion users, it is important to have insights into their trust in brands on WhatsApp, as well as their willingness to disclose personal information to these brands. Using data from a national representative survey, we find that the perceived security, perceived privacy, and perceived socialness of WhatsApp as a platform are positively associated with trusting brands on that messaging platform. In turn, brand trust positively influences consumers' intentions to disclose information to brands on WhatsApp. Finally, these results are also compared with Facebook Messenger; there are significant differences between the two messaging platforms.

Keywords: WhatsApp, brands, trust, self-disclosure, data protection

Instant messaging applications, such as Facebook Messenger and WhatsApp, have become important channels for private interactions with friends and family. With this popularity also came an increased interest in appropriating these channels for commercial purposes. Facebook, Inc., has recently launched WhatsApp for Business. As of January 2020, brands (e.g., commercial companies, political candidates, NGO's) are able to initiate a private chat conversation with consumers through the direct messaging tool WhatsApp, just like these consumers would do with friends or family. This chat conversation can either take place with an employee of the brand or with a chatbot (i.e., a conversational agent that is programmed to communicate with people through natural language, and when requested, can automatically execute specific commands; Zarouali, Van den Broeck, Walrave, & Poels, 2018).

Brahim Zarouali: b.zarouali@uva.nl
Anna Brosius: A.Brosius@uva.nl
Natali Helberger: N.Helberger@uva.nl
Claes H. de Vreese: C.H.deVreese@uva.nl
Date submitted: 2020-05-04

This development has some potential benefits for commercial parties, such as providing consumers with quick responses, the opportunity to tap into new audiences (such as younger consumers that are very active on messaging platforms), and the convenience to interact with consumers in a conversational way (Araujo et al., 2019). However, there are also potential harms to consumers and society. Specifically, given the private nature of the WhatsApp environment, consumers might not be fully aware of the commercial intentions of these brands. One of the consequences could be that consumers' personal information is sold (to other companies), combined, or repurposed without them being aware of it. This raises a potential conflict with fundamental rights to data protection and privacy and also consumer protection law, and rules about unfair commercial practices. In addition, given that these chats with brands on WhatsApp are private one-on-one conversations (thus, invisible to the broad public), it is virtually impossible to monitor what type of information brands communicate to consumers, thereby creating an entirely new dimension of enforcement problems. This creates an environment which could potentially be more conducive to (manipulative, inappropriate, etc.) persuasion attempts by brands or other institutions to alter consumers' opinions for their own benefit (e.g., financial profit, political votes), while this goes largely unnoticed by regulatory bodies because of the private nature of the chat.

Based on this reasoning, a thorough understanding of people's perceptions of and intentions toward WhatsApp brands is needed. Based on structural equation modeling (SEM), this study presents and tests a research model in which brand trust is the central construct. It is one of the most important elements in establishing consumer–brand relationships (Ambler, 1997; Delgado-Ballester, Munuera-Alemán, & Yagüe-Guillén, 2003; Garbarino & Johnson, 1999), and thus an important factor in determining consumers' intentions about brands on WhatsApp. As such, the model explores the extent to which perceptions about WhatsApp (i.e., perceived socialness, security, and privacy) are related to brand trust, and how brand trust is associated with the intention to disclose information to those brands on that platform. The data collection was conducted shortly before the launch of WhatsApp for Business; therefore, this study provides an early exploration of the importance of perceptions and trust beliefs in determining future disclosing intentions. In addition, we aimed to explore whether the hypothesized model also applies to other messaging platforms. To achieve this, the model was also estimated among a Facebook Messenger subsample, and compared with the WhatsApp subsample by means of multigroup analyses in SEM. This procedure allows us to evaluate whether the hypothesized model is robust across different contexts.

Theoretical Framework

Predictors of Brand Trust

Conceptualizing Brand Trust

Trust, generally speaking, is the result of a truster's evaluation of how likely the trustee will behave according to the truster's expectations (Baier, 1986; Bauer, 2014; Coleman, 1990). Trust has received considerable attention in several disciplines such as psychology, sociology, economics, communication science, and marketing. For brands, it refers to a psychological state interpreted in terms of having "confidence" in a positive outcome on the part of the brand (Delgado-Ballester et al., 2003). Put differently, it comprises the attribution of good intentions to the brand in relation to the consumers' interests and welfare. Trust is one of

the most important elements in establishing consumer–brand relationships (Ambler, 1997), and is shaped by consumers' prior experiences and interactions with the brand (Garbarino & Johnson, 1999).

On WhatsApp, it is important to differentiate between trust in the brand WhatsApp (as a platform), and trust in external brands that use WhatsApp to communicate with consumers, which is the focus of this study. In this regard, *brand trust* entails having confidence that a brand reliably does "the right thing" on WhatsApp. It refers to a set of expectations that need to be fulfilled by the brand on WhatsApp, and these expectations can differ per individual. In the literature *perceived privacy* and *perceived security* of an online environment are identified as key determinants of trust in commercial actors (Belanger, Hiller, & Smith, 2002; Flavián & Guinalíu, 2006; Riquelme & Román, 2014). In addition to these two factors, and given how online environments are increasingly introducing social cues in the consumer–brand online relationship (for a more social consumer experience), the *perceived socialness* of the online setting has been highlighted as another important factor that has a positive influence on trust in commercial parties (Hammick & Ju, 2018; Lu, Fan, & Zhou, 2016). These three perceptions could also be highly relevant in the case of WhatsApp: A recent study on the public perceptions of WhatsApp found that the words *social*, *privacy*, and *security* were often associated with the app (Caetano et al., 2018). Based on this line of reasoning, the next section will address how these three perceptions of the messaging app (i.e., *perceived socialness*, *perceived security*, and *perceived privacy*) could determine a user's trust in a brand on WhatsApp. In addition, we also focus on information privacy concerns as an additional variable that might explain some variation of brand trust (see Figure 1).

Perceptions of the App

Studies supporting the Computers Are Social Actors (CASA) paradigm (Reeves & Nass, 1996) have largely established that humans tend to treat websites and as social entities if they contain social-like cues (Sah & Peng, 2015). In this line of research, perceived socialness is an important element of trust (Gefen & Straub, 2004). This socialness has a positive influence on relationship commitment because it can contribute to the relational bond between consumers and brands (Hammick & Ju, 2018). The latter stems from the idea that increasing perceived socialness of a medium or channel is essential to create a sustainable trust relationship between truster and trustee (Seeger & Heinzl, 2018). Research shows that trust can be enhanced by social cues that a brand displays on a website (i.e., personal, sociable, and sensitive human contact of the website; Gefen & Straub, 2004; Lu et al., 2016). WhatsApp can be considered a channel with social richness, because its main purpose is interaction with contacts that one knows personally, such as friends, family, and acquaintances—or, in other words, interpersonal communication with close ties. Messages can be more personalized with photos and video or voice messages. This social nature of WhatsApp use may be generalized by users, who may perceive any interaction on the platform as more social than on other platforms, which are used less for interpersonal communication. Therefore, we argue that *perceived socialness* will increase trust in brands on WhatsApp.

In addition to perceived socialness, perceived security is an important feature. Perceived security refers to consumers' beliefs that their personal information (i.e., personal data) will not be viewed, stored, and used by unauthorized third parties (Flavián & Guinalíu, 2006). Ranganathan and Ganapathy (2002) found that security is one of the key dimensions of business-to-consumer (B2C) website design. Prior research found it to be positively related to trust in websites (Flavián & Guinalíu, 2006; Kim, Ferrin, & Rao, 2008) and more

specifically in social networking sites (Shin, 2010). When it comes to specific security enforcement mechanisms, Chellappa and Pavlou (2002) proposed encryption as an important antecedent of information security. As such, consumer perceptions of security enforcement principles of an app are positively associated to trust in commercial parties (Riquelme & Román, 2014). This is important element for investigating WhatsApp, as it uses end-to-end encryption (and informs all users of this security principle at the beginning of every chat). We expect *perceived security* of the messaging app to positively influence brand trust.

Finally, consumer's trust in brands might also depend on their privacy perceptions of the messaging app. Although related, perceived security and perceived privacy are conceptually distinct (Flavián & Guinalíu, 2006; Riquelme & Román, 2014; Shin, 2010). The former refers to whether personal data are secure from unauthorized third parties, while the latter indicates the extent to which a platform or technology is perceived to compromise privacy (Shin, 2010). The concept of privacy also includes informational privacy in the form of the right to data protection, and communicational privacy (i.e., the right to communicate with others in private, undisturbed by third parties; Koops et al., 2016). As such, perceived privacy reflects the degree to which consumers believe that a platform maintains the ability to communicate with friends in private (Chellappa, 2008). We know from previous studies that the extent to which users feel that social platforms protect their privacy has a positive influence on their trust of the site (e.g., Chang, Liu, & Shen, 2017; Shin, 2010). M. Y. Wang, Zhang, Zhou, and Lai (2019) found similar results in the context of private (chat) messaging apps. Hence, we expect that that perceived privacy is positively related to brand trust on WhatsApp.

Based on the reasoning above, we hypothesize that these three general perceptions—socialness, security, and privacy—of social messaging apps will have a significant influence on consumers' trust in the brands that are active on WhatsApp for commercial purposes:

H1: Perceived socialness of WhatsApp is positively associated with consumers' trust in a brand on the messaging app.

H2: Perceived security of WhatsApp is positively associated with consumers' trust in a brand on the messaging app.

H3: Perceived privacy of WhatsApp is positively associated with consumers' trust in a brand on the messaging app.

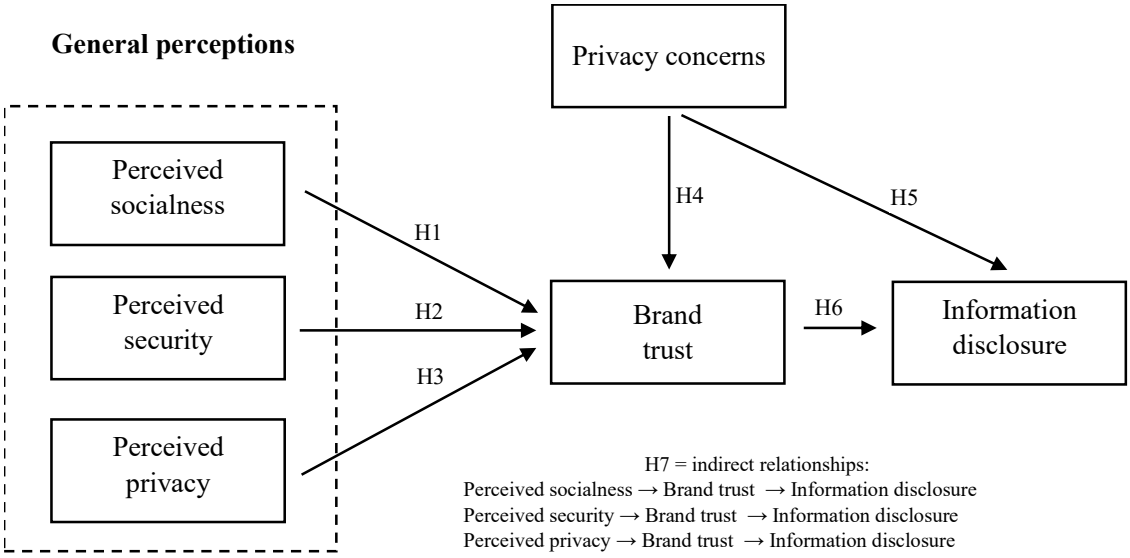

Figure 1. Visual depiction of the hypothesized relationships.

General Privacy Concerns

An important barrier that brands may face when interacting with consumers through messaging apps is their informational privacy concern. Westin (1967) defines informational privacy as "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 7). In the area of online marketing, it is commonly interpreted as a general concern for unauthorized collection and use of one's personal data by brands, as well as selling this data to other commercial actors (H. Wang, Lee, & Wang, 1998). In many studies, a negative relationship was found between privacy concerns and trusting beliefs in general (e.g., Bansal, Zahedi, & Gefen, 2010; Eastlick, Lotz, & Warrington, 2006; Kim et al., 2008; Malhotra, Kim, & Agarwal, 2004). That is, people's tendency to worry about informational privacy negatively influences how they perceive specific situations in which online commercial actors interact with them (Bansal et al., 2010; Kelly, Kerr, & Drennan, 2017; Malhotra et al., 2004). More specifically, a recent study found that privacy concerns are a major factor when it comes trust in social communication on instant messaging apps (Cheng, Fu, & de Vreede, 2017). Based on this, we expect a similar relationship: General privacy concerns will be negatively related to trust in the sender of a brand message on WhatsApp. We propose the following:

H4: Consumers' informational privacy concerns is negatively associated with their trust in a brand on WhatsApp.

Information Disclosure

In this study, we also aim to investigate consumers' willingness to disclose personal information about themselves to these brands, often referred to as self-disclosure, as trust plays a fundamental role in this process (Taddei & Contena, 2013; Waldman, 2016). Self-disclosure is the process of intentionally

revealing personal information about oneself to others (e.g., to people, companies; Derlega, 1993). When people disclose personal information via direct messaging apps, it is usually directed to friends and family. However, with brands increasing their presence on social platforms, it yields some serious concerns about people's self-disclosure to these commercial parties (Walrave, Utz, Schouten, & Heirman, 2016). An increase in self-disclosure means that brands have more access to personal data about their target audiences that could serve their commercial, political, or financial interests (Walrave et al., 2016).

Trust and privacy concerns are two of the most important factors in deciding whether or not to disclose information (e.g., Bansal et al., 2010; Heirman, Walrave, Ponnet, & Gool, 2013; Kehr, Kowatsch, Wentzel, & Fleisch, 2015; Liu, Min, Zhai, & Smyth, 2016; Metzger, 2004; Posey, Lowry, Roberts, & Ellis, 2010). They are a central concept of social exchange theory (Roloff, 1981), which posits that people conduct a mental trade-off (i.e., weighing the costs and benefits) in deciding whether to engage in transactions with others. If the benefits outweigh the costs, then the individual is likely to engage in an exchange relationship in which self-disclosure takes place (Liu et al., 2016; Metzger, 2004). As for trust, it has been identified as the element that binds social exchanges (Posey et al., 2010). Although most research on trust centers around interpersonal communication, similar risk-benefit dynamics have been found regarding information disclosure to commercial actors (Culnan & Armstrong, 1999; Jarvenpaa, Tractinsky, & Vitale, 2000; Metzger, 2004). Thus, when individuals trust online companies and brands (costs < benefits), they are more willing to disclose personal information (Schoenbachler & Gordon, 2002). Privacy concerns, on the other hand, are a major factor that prevent consumers from releasing information online (Kehr et al., 2015; Liu et al., 2016; Malhotra et al., 2004). Individuals maintain and coordinate certain privacy boundaries (Petronio, 2002). These boundaries also depend on the perceived costs and benefits of self-disclosure: When people perceive the (privacy) costs of disclosing to be much higher than the benefits, they may be more likely to refrain from disclosing any information about themselves to the communication partner (and vice versa; Posey et al., 2010). Based on this argumentation, we expect the following hypotheses:

H5: Consumer' informational privacy concerns are negatively associated with their intention to disclose information to a brand on WhatsApp.

H6: Consumer' brand trust is positively associated with their intention to disclose information to a brand on WhatsApp.

Mediating Role of Trust

In addition to the aforementioned direct effects in our model, we can also address brand trust as an important mediating variable in increasing consumers' willingness to self-disclose (Chou, Teng, & Lo, 2009; Heirman et al., 2013). In other words, perceptions of WhatsApp (i.e., perceived socialness, perceived privacy, and perceived security) might affect trust in a brand on that messaging service (see H1–H3), and in turn, these trust beliefs might influence their intention to disclose information to the brand on WhatsApp. This mediated relationship among platform perceptions, trust, and behavioral intentions has been well established in the literature (e.g., Hong & Cha, 2013; Kehr et al., 2015; Singh & Sinha, 2020; Zboja & Voorhees, 2006). More precisely, perceptions of online platforms might be an important factor in determining people's willingness

self-disclose, as a result of an increase in trust (Joinson, Reips, Buchanan, & Schofield, 2010; Taddei & Contena, 2013). Based on this line of reasoning, we formulate the following hypothesis:

H7: Brand trust mediates the relationship among platform perceptions (i.e., socialness, privacy, and security) and the intention to disclose information to a brand on WhatsApp.

WhatsApp Versus Facebook Messenger

Finally, this study also explores whether there are differences between WhatsApp and Facebook Messenger in relation to the hypothesized model. In other words, in an effort to test whether the hypothesized mechanisms also apply in other contexts, we test the hypothesized model (see Figure 1) not only for WhatsApp but also for Facebook Messenger. Though both messaging platforms are seemingly similar and part of the same technology company (Facebook, Inc.), research has shown that they are used to fulfill different needs (Karapanos, Teixeira, & Gouveia, 2016; Nouwens, Griggio, & Mackay, 2017; Waterloo, Baumgartner, Peter, & Valkenburg, 2018). WhatsApp is generally used as a private channel for personal self-expression with close contacts, whereas Facebook Messenger also revolves around communication with weaker ties (Karapanos et al., 2016; Waterloo et al., 2018). As such, Nouwens et al. (2017) found that users draw boundaries between these apps in terms of membership rules (who belongs to the app), perceived purpose (what the app is for), and emotional connotations (how they feel to other users).

Recently, findings show that Facebook is the least trusted company in terms of safeguarding personal data (compared with other big tech companies such as Google and Apple; Vanian, 2018). An important reason for this distrust might be the company's involvement in widely publicized scandals, such as the Cambridge Analytica affair (Gupta, 2019). Since people's trust in specific brands depends on the perceptions they have about the safety of the overall platform environment (Harrison McKnight, Choudhury, & Kacmar, 2002), brands using Facebook Messenger for their communication with consumers could suffer from the platform's negative reputation (Van den Broeck, Zarouali, & Poels, 2019). Although WhatsApp is part of the same company, survey results showed that more than half of the U.S. population did not know that WhatsApp is owned by Facebook (DuckDuckGo, 2018). Therefore, people might hold different perceptions about both platforms, and as such, have different levels of trust and self-disclosure toward brands using the messaging service on those platforms. Based on this, we formulate the following research question:

RQ1: Are there differences in the hypothesized relationships (see H1–H7) between WhatsApp and Facebook Messenger?

Methodology

Sample and Data

We used data from a larger panel survey, which was distributed among a representative sample of the (location blinded for peer review) population by the market research company IPSOS. The larger survey focused on the impact of personalized communication and algorithms on society. The survey was carried out online in December 2019, which was one month before the official launch of WhatsApp for Business.

The total sample size was *N* = 1,289, with an overall response rate of 61%. The respondents had a mean age of 52.18 years (*SD* = 15.71 years), and 46% of them were women. Education level was recoded into three categories: low, medium, and high levels of education. Around 27% had a lower education level, 50% had medium levels of education, and 23% had a higher education level.

For the first part of this study (i.e., H1–H7), we analyzed only the data of those respondents that received questions about their perceptions of WhatsApp (*n* = 645). This means that respondents who received questions about their perceptions of Facebook Messenger were not included in this initial analysis. Because this subsample was randomly drawn, the distribution of the demographic variables is highly similar to the total sample (see Table 1 for more detailed demographic information). For the analyses of RQ1, we used the full data set (*N* = 1,289) to conduct multigroup analyses (i.e., comparing both samples).

Table 1. Demographic Overview of the Total Sample and Across the Subsamples.

	FB Messenger subsample	WhatsApp subsample	Total sample	χ^2
Age categories				.05 (*ns*)
18–34 years	18%	18%	18%	
35–54 years	37%	37%	37%	
55+ years	46%	45%	45%	
Gender				1.80 (*ns*)
Female	44%	48%	46%	
Male	56%	52%	54%	
Education				4.40 (*ns*)
Low	25%	30%	27%	
Moderate	52%	48%	50%	
High	23%	22%	23%	

Note. Chi-square test of independence was conducted; *ns* = not significant.

Data Collection Procedure

After filling out some demographic questions, a random split run was included in the survey. Respondents received the same questions, but about a different messaging platform. They were either presented the questions in the context of WhatsApp, or in the context of Facebook Messenger. Furthermore, respondents were also shown a fictitious example of a brand message via private messaging, either embedded in WhatsApp or Facebook Messenger (depending on which questions they received; see Appendix). These examples consisted of an illustration of a smartphone screen showing either a conversation with a fictious brand on WhatsApp, or on Facebook Messenger. These stimuli helped the respondents to understand what kind of brand communication we were referring to. This is important to ensure the validity of the results.

Measures

To measure perceived socialness, we used five statements on a 7-point Likert scale from Gefen and Straub (2004). The answer options ranged from 1 (*strongly disagree*) to 7 (*strongly agree*). Perceived security was measured with two items on the same 7-point agreement scale, following Hartono, Holsapple, Kim, Na, and Simpson (2014). Perceived privacy was measured by using an instrument developed by Dinev et al. (2012), which consists of three items with answer options ranging from 1 (*strongly disagree*) to 7 (*strongly agree*). To measure respondents' privacy concerns, we used a five-item instrument developed by Baek and Morimoto (2012) that we adapted. The scale ranged from 1 (*totally disagree*) to 7 (*totally agree*). To assess brand trust, we used a validated instrument developed by Walsh, Beatty, and Shiu (2009), consisting of five items. The items were measured on a 7-point Likert scale ranging from 1 (*strongly disagree*) to 7 (*strongly agree*). The intention to self-disclose was measured with three bipolar adjectives derived from Malhotra et al. (2004), assessed on a 7-point semantic deferential. The correlations between the main variables are presented in Table 2, together with their means and standard deviations. For a full overview of all the items used in this study, see Table 3.

It is important to note that the wordings of the items of brand trust and self-disclosure are using different tenses. The reason for this is because the survey was conducted in December 2019, which is before WhatsApp for Business had launched (January 2020). Therefore, participants had no prior experience with brands on WhatsApp. That is why these items have a slightly different grammatical structure (e.g., "would") than the other items.

Table 2. Means, Standard Deviations (SDs), and Correlation Matrix.

		WhatsApp subsample							FB Messenger subsample						
Construct		*M*(*SD*)	1	2	3	4	5	6	*M*(*SD*)	1	2	3	4	5	6
1	PSO	[a]4.57(1.32)	–						[b]3.36(1.50)	–					
2	PSE	[a]4.02(1.26)	.44	–					[b]3.02(1.40)	.57	–				
3	PPR	[a]4.27(1.36)	.46	.67	–				[b]3.15(1.52)	.59	.68	–			
4	BTR	[a]3.16(1.37)	.52	.54	.54	–			[b]2.73(1.35)	.47	.58	.46	–		
5	IND	[a]3.03(1.79)	.46	.38	.39	.66	–		[b]2.25(1.41)	.39	.42	.43	.69	–	
6	PCO	[a]4.95(1.23)	−.03	−.28	−.33	−.13	−.08	–	[a]4.96(1.20)	−.09	−.27	−.29	−.20	−.17	–

Note. PSO = perceived socialness; PSE = perceived security; PPR = perceived privacy; PCO = privacy concerns; BTR = brand trust; IND = intention to disclose. Means in the same row with a different superscript differ significantly ($p < .05$).

Results

Analytical Strategy

The hypothesized model was tested with SEM using lavaan in R (Rosseel, 2012). Based on a multivariate normality test using the package MVN in R (Korkmaz, Goksuluk, & Zararsiz, 2014), we calculated Mardia's multivariate skewness and kurtosis coefficients. This revealed that the distribution of the entire sample is normal, which allows for the use of maximum likelihood estimation in SEM. The analysis

consists of different steps. First, we built a measurement model and examined whether the manifest variables provided a reliable reflection of the latent variables. Then, we estimated a structural model to test the relations among the latent variables (i.e., hypothesis testing), followed by specifying and testing the indirect relationships in the model. To infer indirect relationships, we used the Sobel test approach. Finally, we conducted multigroup analyses to test the model across the two different subsamples (WhatsApp and FB Messenger) and explore differences in path estimates.

Measurement Model

As a first step, we aimed to confirm adequate support for the measurement models of both subsamples to establish a proper relationship between the manifest variables and their corresponding latent constructs. Based on a confirmatory factor analysis (CFA) with maximum likelihood estimation, we found that the model for the WhatsApp subsample, $\chi^2(215) = 677.91$, $p < .001$, comparative fit index (CFI) = 0.96, Tucker–Lewis index (TLI) = 0.95; standardized root-mean-square residual (SRMR) = 0.027, root-mean-square error of approximation (RMSEA) = 0.058, 95% confidence interval (CI) [0.054, 0.062], as well as the Facebook Messenger subsample, $\chi^2(215) = 686.80$, $p < .001$, CFI = 0.97, TLI = 0.96, SRMR = 0.034, RMSEA = 0.058, CI [0.054, 0.062], had a good fit.

To measure reliability and validity of our model, composite reliability (CR) and average variance extracted (AVE) were estimated in this study (Bagozzi & Yi, 1988). Table 3 presents all these values, together with the Cronbach's alpha's and standardized factor loadings for all items. The standardized loadings for all items in both subsamples were high and statistically significant ($p < .001$), and all Cronbach's alpha values indicate good internal consistency of the scales. It also shows that both CR values (ranging from 0.91 to 0.96) and AVE values (ranging from 0.64 to 0.88) for all constructs exceed the cutoff limits of 0.70 and 0.50, respectively (Bagozzi & Yi, 1988).

Discriminant validity was then tested by comparing the AVE values for any two constructs with the square root of the correlation estimate between these two constructs. If the AVE is higher than the squared correlation estimate, then discriminant validity is demonstrated (Fornell & Larcker, 1981; Hair, Black, Babin, & Anderson, 2014). Both subsamples passed this test for all the constructs in the study.

Table 3. Construct Measurement Summary: Results of Convergent Validity Tests.

	WhatsApp subsample (n = 645)			Facebook Messenger subsample (n = 644)		
Constructs and items	Stand. loading	AVE	CR	Stand. loading	AVE	CR
Perceived socialness (Cronbach's α = 0.94)		0.68	0.91		0.78	0.95
1. There is a sense of human contact in WhatsApp/Facebook Messenger	0.77			0.83		
2. There is a sense of personalness in WhatsApp/Facebook Messenger	0.78			0.81		
3. There is a sense of sociability in WhatsApp/Facebook Messenger	0.82			0.92		
4. There is a sense of human warmth in WhatsApp/Facebook Messenger	0.88			0.95		
5. There is a sense of human sensitivity in WhatsApp/Facebook Messenger	0.86			0.91		
Perceived security (Cronbach's α = 0.92)		0.81	0.91		0.85	0.92
1. My personal information is securely managed in WhatsApp/Facebook Messenger	0.88			0.91		
2. WhatsApp/Facebook Messenger is safe for my personal information	0.92			0.94		
Perceived privacy (Cronbach's α = 0.95)		0.80	0.93		0.88	0.96
1. I feel have enough privacy when using WhatsApp/Facebook Messenger	0.89			0.93		
2. I am comfortable with the amount of privacy I have when using WhatsApp/Facebook Messenger	0.90			0.96		
3. I think my privacy is preserved when I use WhatsApp/Facebook Messenger	0.90			0.93		
Brand trust (Cronbach's α = 0.96)		0.84	0.96		0.83	0.96
1. I would trust a brand on WhatsApp/Facebook Messenger	0.90			0.87		
2. I would have confidence in a brand on WhatsApp/Facebook Messenger.	0.89			0.94		
3. A brand on WhatsApp/Facebook Messenger would have integrity.	0.93			0.92		
4. I can depend on a brand on WhatsApp/Facebook Messenger to do the right thing.	0.92			0.92		
5. A brand on WhatsApp/Facebook Messenger can be relied upon.	0.93			0.92		
Information disclosure (Cronbach's α = 0.93)		0.88	0.93		0.82	0.94
Please specify the extent to which you would share personal information to a brand on WhatsApp/Facebook Messenger:						
1. Unlikely/likely	0.92			0.93		
2. Not probable/probable	0.92			0.94		
3. Unwilling/willing	0.87			0.83		
Privacy concerns (Cronbach's α = 0.90)		0.64	0.90		0.65	0.91
1. I am worried that my personal data may be misused by others.	0.71			0.77		
2. When I am online, I have the feeling that others keep track of what I do.	0.65			0.67		
3. I am afraid that my personal data that I share online is not stored safely.	0.86			0.88		
4. I am afraid that my personal data online is distributed without my permission.	0.88			0.87		
5. I am afraid that my personal data online can be accessed by people I do not know.	0.91			0.87		

Structural (WhatsApp) Model: Testing Hypotheses 1–7

To test H1–H7, a structural model was estimated for the WhatsApp subsample, in which we define the predicted relationships among the latent variables. Table 4 presents the results of the structural model, including its standardized regression coefficients and standard errors. The goodness-of-fit indices indicate a good fit for the model, $\chi^2(218) = 686.27$, $p < .001$, CFI = 0.96, TLI = 0.95, SRMR = 0.029, RMSEA = 0.058, CI [0.053, 0.062]. The explained variance for brand trust was 59% ($R^2 = .59$), and for disclosure intention 43% ($R^2 = .43$). As reported in Table 4, the three variables representing the platform perceptions (i.e., socialness, privacy, and security) are significantly related to brand trust on WhatsApp. Therefore, H1–H3 are supported. Surprisingly, when it comes to privacy concerns, the model revealed neither a significant relationship with brand trust (H4) nor intention to self-disclose (H5). Thus, both hypotheses are rejected. Brand trust has a strong and positive relationship with disclosure intention, which confirms H6.

Table 4. Standardized Path Coefficients Across Both Subsamples.

		WhatsApp subsample (n = 645)		Facebook Messenger subsample (n = 644)	
		Std. path coefficient	*SE*	Std. path coefficient	*SE*
H1	PSO → BTR	0.34***	0.05	0.16***	0.04
H2	PSE → BTR	0.22***	0.11	0.15***	0.08
H3	PPR → BTR	0.20***	0.20	0.15***	0.09
H4	PCO → BTR	−0.01	0.05	−0.03	0.05
H5	PCO → IND	0.04	0.05	−0.05	0.04
H6	BTR → IND	0.76***	0.04	0.67***	0.04
H7	*Direct effects:*				
	PSO → IND	0.11**	0.06	0.08*	0.04
	PSE → IND	−0.04	0.13	−0.06	0.08
	PPR → IND	−0.06	0.10	0.04	0.08
	Indirect effects:				
	PSO → BTR → IND	0.25***	0.05	0.11***	0.03
	PSE → BTR → IND	0.17**	0.11	0.15***	0.07
	PPR → BTR → IND	0.15**	0.09	0.13***	0.06

Note. PSO = perceived social presence; PSE = perceived security; PPR = perceived privacy; PCO = privacy concerns; BTR = brand trust; IND = intention to disclose. *$p < .05$, **$p < .01$, ***$p < .001$.

In H7, we predict that the relationship among the three WhatsApp perception variables (socialness, privacy, and security) would be positively related to information disclosure, through brand trust as the mechanism that underlies the predictive links among these variables. As illustrated in Table 4, only one of the three direct relationships is significant (i.e., perceived socialness), while all indirect paths yield significant values. That means two variables are fully mediated and one variable is partially mediated. Therefore, we conclude that H7 can be accepted.

Multigroup Testing: Answering RQ1

To establish whether there are model-related differences (i.e., path coefficients), various multigroup analyses were performed. We followed prior literature to explore group differences by comparing a series of nested models (e.g., Riquelme & Román, 2014; Teo, Lee, Chai, & Wong, 2009). To compare different groups, we first have to test for measurement invariance to ensure that the items are measuring the same constructs in both samples (Steenkamp & Baumgartner, 1998). This test started with a baseline model (i.e., configural model—M1) and showed an acceptable fit, $\chi^2(430) = 1883.30$, SRMR = .029, RMSEA = .072, CFI = .95, TLI = .94. Then, we assessed a metric invariance model (M2), which assumes intergroup equality of factor loadings (by adding equality constraints to the factor loadings). This M2 model led to an increase in χ^2 of around 49 ($\Delta\chi^2 = 49.18$, $\Delta df = 17$), compared with the configural solution, which is a significant difference ($p < .001$). This means that full metric invariance is not supported.

However, scholars have argued that a partial invariance (i.e., tolerating that some factor loadings can differ across groups) is also acceptable (Byrne, 2009; Steenkamp & Baumgartner, 1998). Therefore, we constrained the three items that were not invariant across the groups (brand trust Item 2, information disclosure Item 3, privacy concerns Item 1—see Table 3 for the item wordings). Based on this, we estimated a partial invariance model (M3), which had a good fit and was not significantly different from the baseline, configural model M1 ($\Delta\chi^2 = 14.61$, $\Delta df = 14$, $p < .41$). Moving on, we assessed scalar invariance, which assumes intergroup equivalence for both factor loadings and items' intercepts. The full scalar model (M4) resulted in a significant change in χ^2 value ($\Delta\chi^2 = 46.23$, $\Delta df = 17$, $p < .001$). We identified and constrained two intercepts that were not invariant across the two groups (information disclosure Item 3, perceived socialness Item 2). By constraining these two items, we estimated a partial scalar model (M5), which was not significantly different from the baseline model ($\Delta\chi^2 = 22.30$, $\Delta df = 15$, $p = .10$). Having established partial scalar invariance, we then proceeded to test structural coefficient differences across groups (RQ1).

To answer RQ1, we first have a look at the regression coefficients for both samples, which can be consulted in Table 4. Based on a visual analysis of this table, we can see that all the significant paths for the WhatsApp subsample are also significant for the Facebook subsample, though the coefficients in the Facebook Messenger group are much weaker. Then, an overall structural model was estimated, and it revealed an acceptable fit with the data, $\chi^2(218) = 692.41$, $p < .001$, CFI = 0.96, TLI = 0.96, SRMR = 0.037, RMSEA = 0.070, CI [0.064, 0.076]. After this, we proceeded with (structural) multigroup analysis, which revealed significant variation in path coefficients across the two subsamples, since the model of total equality of pathways was rejected ($\Delta\chi^2 = 56.07$, $\Delta df = 12$, $p < .001$). To inspect this significant invariance in paths in more detail, we conducted a series of one degree of freedom pairwise comparisons of both subsamples for each hypothesized path (see H1–H6). At each time, we compared a baseline model with a nested model, in which a parameter (i.e., a specific path) was constrained. The results of these pairwise analyses are reported in Table 5.

Table 5. Multigroup Comparison of Path Coefficients Among the WhatsApp and FB Messenger Subsample.

Path (whose equality constraint was released)	χ^2	$\Delta\chi^2$	*p* value
Baseline	1,976.2		
PSO → BTR	1,949.1	27.18	$p < .001$
PSE → BTR	1,966.7	9.59	$p < .01$
PPR → BTR	1,967.7	8.51	$p < .01$
PCO → BTR	1,976.0	0.25	$p = .62$
PCO → IND	1,975.8	0.40	$p = .53$
BTR → IND	1,964.4	11.86	$p < .001$

Note. PSO = perceived social presence; PSE = perceived security; PPR = perceived privacy; PCO = privacy concerns; BTR = brand trust; IND = intention to disclose.

In this table, a significant χ^2 value difference for the two models indicates that the path coefficient is statistically different across the two subsamples (Byrne, 2009; Riquelme & Román, 2014; Teo et al., 2009). The effects of perceived socialness ($\beta_{WA} = .34$ vs. $\beta_{FB} = .16$, $\Delta\chi^2 = 27.18$, $p < .001$), perceived security ($\beta_{WA} = .22$ vs. $\beta_{FB} = .15$, $\Delta\chi^2 = 9.59$, $p < .01$) and perceived privacy ($\beta_{WA} = .20$ vs. $\beta_{FB} = .15$, $\Delta\chi^2 = 8.51$, $p < .01$) are significantly stronger in the WhatsApp group than in the Facebook group. We found no significant difference between both groups in the effect of privacy concerns on brand trust ($\beta_{WA} = -0.01$ vs. $\beta_{FB} = -0.03$, $\Delta\chi^2 = 0.40$, $p = .53$) and on intention to self-disclose ($\beta_{WA} = .04$ vs. $\beta_{FB} = -.05$, $\Delta\chi^2 = 0.40$, $p = .53$). Finally, analyses revealed a much larger effect of brand trust on intention to self-disclose in the WhatsApp condition than in the Facebook condition ($\beta_{WA} = .76$ vs. $\beta_{FB} = .67$, $\Delta\chi^2 = 11.86$, $p < .001$). In sum, all the direct paths, except those related to privacy concerns, are significantly larger in the WhatsApp group compared with the Facebook group.

Regarding the indirect effects (see Table 4), the path of perceived socialness to intention to self-disclose via brand trust was significant in both groups (*indirect effect* $_{WA} = .25$, $p < .001$; *indirect effect* $_{FB} = .11$, $p < .001$), but was much more pronounced in the WhatsApp condition. The two other indirect effects in Table 4 are also significant in both subsamples: perceived security (*indirect effect* $_{WA} = .17$, $p < .01$; *indirect effect* $_{FB} = .15$, $p < .001$) and perceived privacy (*indirect effect* $_{WA} = .15$, $p < .001$; *indirect effect* $_{FB} = .13$; $p < .001$) on intention to self-disclose via brand trust, but instead of seeing large differences across the two groups, they were only slightly more pronounced in the WhatsApp group.

Discussion

This study identified and tested a research model (see Figure 1) in which brand trust operates as an underlying mechanism for why consumers might be willing to disclose their personal information to brands on WhatsApp. Results revealed a well-fitting model, which shows that consumers' perceptions of *socialness*, *security* and *privacy* in WhatsApp are related to increased trust in brands communicating via this messaging app. Furthermore, we found that brand trust also mediates the effect of these perceptions on consumers' intention to disclose personal information to a brand on WhatsApp. Having more favorable perceptions about WhatsApp increases people's trust in brands on WhatsApp, which in turn increases their intention to disclose personal information to these brands.

Besides WhatsApp, we also explored whether the hypothesized model fit in a different context (i.e., Facebook Messenger). After having established measurement invariance (i.e., partial scalar invariance), we found significant differences showing that the relations among the main variables in the research model are different across the two samples. More precisely, all hypothesized relationships in the model (except for those related to privacy concerns) were significantly stronger in the WhatsApp group, compared with the Facebook Messenger group. In addition, the WhatsApp model had a better fit to the data than the Facebook Messenger model. Based on the descriptive results, we also conclude that consumers have less favorable perceptions about Facebook Messenger, as well as lower trust in and intention to disclose information to brands on Facebook Messenger (as compared with WhatsApp). In brief, we were able to apply the hypothesized WhatsApp model in a different context (while still preserving an acceptable fit), although it has to be noted that the WhatsApp group had more favorable descriptive results, stronger psychometric properties (for the model), and stronger intervariable relationships (compared with the Facebook group).

Our study makes an incremental theoretical contribution to the limited literature on brand communication via WhatsApp and Facebook Messenger. When it comes to platform perceptions (i.e., socialness, security, and privacy; e.g., Belanger et al., 2002; Flavián & Guinalíu, 2006; Gefen & Straub, 2004; Lu et al., 2016), we showed that they operate through direct (on trust) and indirect effects (on disclosure intention) in a private messaging setting. These results make a valuable contribution to the development of theory on how environmental perceptions affect brand responses and behavioral intentions. With respect to brand trust, we showed its importance for communication on WhatsApp: Trust is influenced by platform perceptions and can be theorized as a meaningful mediator through which these platform perceptions affect intentions to disclose information to brands (see also Culnan & Armstrong, 1999; Jarvenpaa et al., 2000; Metzger, 2004). Thus, it seems that brand trust plays a pivotal role in establishing consumer–brand relationships in WhatsApp (see also Ambler, 1997; Delgado-Ballester et al., 2003).

Contrary to expectations, privacy concerns had an influence neither on brand trust nor on one's intention to self-disclose on WhatsApp. As argued by Taddicken (2014), who found that privacy concerns hardly impact self-disclosure in the social web, it might be important to distinguish between public self-disclosure and self-disclosing behavior within environments where users feel safe from privacy invasion. Based on the descriptive results (see Table 2), we found that WhatsApp is perceived to be a relatively private environment, which might explain the "limited" influence of privacy concerns. However, it would be useful to further investigate this in future studies.

Additionally, the current findings also show differences between WhatsApp and Facebook messenger as platforms of trust. Consumers hold different perceptions about the two messaging apps. Specifically, perceptions toward Facebook Messenger are less favorable, which is in line with previous research (see, e.g., Gupta, 2019; Van den Broeck et al., 2019; Vanian, 2018), and may be due to the lack of knowledge about the shared ownership of both messaging apps (DuckDuckGo, 2018). Such different perceptions might result in different levels of brand trust and intention to self-disclose. In other words, the way consumers evaluate and process interactions with brands might not be invariant across messaging services, but instead, depend on the platform in which the persuasion attempt takes place.

These results have several relevant implications, both for practice and policy. For practitioners (e.g., marketeers, advertisers, brand managers), WhatsApp could be an important and strategic tool to interact with customers (more so than Facebook Messenger). By creating a business account on this popular instant messaging platform, brands could capitalize on the platform's perceptions of socialness, privacy, and security to increase consumers' brand trust, which in turn will translate into a higher willingness to share information with brands. Thus, to improve their marketing strategy, brands could create a business account on WhatsApp (which also provides helpful information for consumers, such as address, website, etc.), and subsequently, offer consumers the opportunity to interact and participate with the brand by means of direct messaging. Some examples of consumer–brand interactions on WhatsApp could involve customer service (e.g., help consumers with their questions by providing quick customer support via chat), promotional offerings (e.g., provide consumers special deals or coupons via chat), customer feedback (e.g., ask consumer for feedback and reviews via chat to get quick and valuable business insights), or updates and reminders (e.g., send updates about the status of an order directly via chat). Most of these consumer–brand interactions can either be done manually (i.e., a person replying to all the messages in a quick and efficient way), or alternatively, in an automated way (i.e., creating a chatbot that responds immediately to every prompt—see Zarouali et al., 2018). Based on our findings, we can conclude that such interactions via WhatsApp, which is an app that is generally used for private conversations, could tap into consumers' feelings of *socialness*, *privacy,* and *security*. These feelings can contribute to an increased brand trust and intention to self-disclose among target audiences, which are important ingredients in establishing strong and long-lasting consumer–brand relationships.

However, in spite of the potential benefits for brands, there are also concerns from a (policy-based) data protection perspective. To the extent that users *do* trust brands that use WhatsApp as a communication channel, such commercial uses of WhatsApp can, without additional information and transparency for the customer, potentially create a false feeling of security. WhatsApp may guarantee a certain level of security and confidentiality of the communication due to encryption, and it also requires its Business users to meet legal obligations, including those arising from the General Data Protection Regulation (GDPR; for services offered in Europe).[1] Having said so, these "guarantees" only apply to the use of WhatsApp for the purpose of communicating with potential customers.[2] WhatsApp exercises no control whatsoever over the use of the personal data that consumers share *after* the communication. Further research would be needed to ascertain whether consumers are aware of the different levels of data processing (processing of personal data in the context of communication via WhatsApp, and further commercial uses of data gained as a result of that communication). It is worth noting that where WhatsApp is used as a means for businesses to communicate with consumers, not only the GDPR is relevant, but also consumer law, for example in the form of the

[1] See WhatsApp Business Terms of Service (https://www.whatsapp.com/legal/business-terms/?lang=en).

[2] "To the extent your customers are located in the European Region and the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') applies to your processing of any Personal Data (as that term is defined in the GDPR) contained within Customer Data, you are the data controller selecting the message recipients and instructing WhatsApp, *for the duration of these Business Terms,* to process such Personal Data on your behalf as your data processor pursuant to these Business Terms to deliver Company's messages to its customers" (emphasis added). WhatsApp Business Terms of Service, section 7 (https://www.whatsapp.com/legal/business-terms/?lang=en).

provisions on unsolicited communication[3] and unfair commercial practices.[4] Another question that arises from this study and that merits further (legal) research is whether the fact that users seem to trust brands using WhatsApp triggers additional obligations regarding the confidentiality of information on the side of WhatsApp, once an amended ePrivacy Directive[5] is expanded to also cover services such as WhatsApp and Facebook. The findings from this study, and the fact that WhatsApp's commercial dealings with businesses may benefit from the trust that consumers have in WhatsApp as a communication platform, could be an additional consideration in that context. On a more practical, enforcement level, the fact that businesses use (encrypted) WhatsApp communication services to engage with potential customers can also pose a challenge for regulatory authorities when enforcing data protection and consumer protection rules.

Finally, this study has a number of limitations that open up pathways for future research. First, we did not measure attitude or familiarity toward the messaging app (WhatsApp and Facebook Messenger). As a result, we could not control for potential confounding effects of prior attitudes and experiences with both platforms. People are likely to have different attitudes toward both platforms, so future research could test how prior attitudes toward the app might impact the effectiveness of marketing communication via private messaging apps. Second, we rely on self-reported survey data and reports of *intentions* to self-disclose. However, such intentions might not always translate into actual behavior. Our research nevertheless provides a starting point for future research, which could, for example, test these findings in a real-life context and measure actual information disclosure toward brands that communicate on WhatsApp or other messaging platforms. Third, future studies should scrutinize the terms of use and privacy policies of WhatsApp vis-à-vis consumers, and Business users, and the extent to which the trust of consumers toward

[3] Art. 7 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('E-Commerce Directive'). According to Art. 7 of the E-Commerce Directive, unsolicited commercial communication (also referred to as "spam") must be in any event clearly identifiable as such. In addition, member states must ensure the availability of opt-out registers, in which natural persons not wishing to receive such commercial communications can register themselves. Member states can also decide to ban unsolicited commercial communication.

[4] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149, 11.6.2005.

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ('ePrivacy Directive'), OJ L 201, 31.7.2002. As to the current state of the procedure regarding the revision of the ePrivacy and possible extension to services such as Whatsapp, see Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Progress report, 23 November 2020, Brussels, https://data.consilium.europa.eu/doc/document/ST-13106-2020-INIT/en/pdf

brands using WhatsApp is actually justified—for example, because of extra safeguards that WhatsApp may, or may not, undertake to protect the privacy of consumers. Moreover, the scope of this article did not allow us to engage in an in-depth assessment of the current practices of using WhatsApp for Business under current and future data protection and consumer law. Based on this study, we suggest that doing so might be useful and necessary.

References

Ambler, T. (1997). How much of brand equity is explained by trust? *Management Decision*, *35*(4), 283–292. doi:10.1108/00251749710169666

Araujo, T., van Zoonen, W., & ter Hoeven, C. (2019). *Automated 1-2-1 communication*. Amsterdam, The Netherlands: SWOCC

Baek, T. H., & Morimoto, M. (2012). Stay away from me: Examining the determinants of consumer avoidance of personalized advertising. *Journal of Advertising*, *41*(1), 59—76. doi:10.2753/JOA0091-3367410105

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74–94. doi:10.1007/BF02723327

Baier, A. (1986). Trust and antitrust. *Ethics, 96*(2), 231–260. doi:10.1086/292745

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

Bauer, P. C. (2014). Conceptualizing and measuring trust and trustworthiness. *Committee on Concepts and Methods Working Paper Series, 61*, 1–27. doi:10.2139/ssrn.2325989

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems, 11*(3), 245–270. doi:10.1016/S0963-8687(02)00018-5

Byrne, B. M. (2009). *Structural equation modeling with AMOS: Basic concepts, applications, and programming* (2nd ed.). New York, NY: Routledge.

Caetano, J. A., Magno, G., Cunha, E., Meira, W., Jr., Marques-Neto, H. T., & Almeida, V. (2018). *Characterizing the public perception of WhatsApp through the lens of media.* ArXiv:1808.05927 [Cs]. Retrieved from http://arxiv.org/abs/1808.05927

Chang, S. E., Liu, A. Y., & Shen, W. C. (2017). User trust in social networking services: A comparison of Facebook and LinkedIn. *Computers in Human Behavior, 69*, 207–217. doi:10.1016/j.chb.2016.12.013

Chellappa, R. K. (2008). *Consumers' trust in electronic commerce transactions: The role of perceived privacy and perceived security*. Unpublished paper. Retrieved from https://www.semanticscholar.org/paper/Consumers-'-Trust-in-Electronic-Commerce-%3A-The-Role-Chellappa/7e2fbad4fa4877ea3fd8d197950e335d59ebeedf.

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management, 15*(5/6), 358–368. doi:10.1108/09576050210447046

Cheng, X., Fu, S., & de Vreede, G. J. (2017). Understanding trust influencing factors in social media communication: A qualitative study. *International Journal of Information Management, 37*(2), 25–35. doi:10.1016/j.ijinfomgt.2016.11.009

Chou, Y., Teng, C., & Lo, S. (2009). Mutual self-disclosure online in the B2C context. *Internet Research, 19*(5), 466–478. doi:10.1108/10662240910998878

Coleman, J. S. (1990). *Foundations of social theory*. Cambridge, MA: Harvard University Press.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104–115. doi:10.1287/orsc.10.1.104

Delgado-Ballester, E., Munuera-Alemán, J. L., & Yagüe-Guillén, M. J. (2003). Development and validation of a brand trust scale. *International Journal of Market Research, 45*(1), 1–18. doi:10.1177/147078530304500103

Derlega, V. J. (Ed.). (1993). *Self-disclosure*. Newbury Park, CA: SAGE Publications.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22*(3), 295—316. doi:10.1057/ejis.2012.23

DuckDuckGo. (2018, October 18). *Most Americans aren't aware that Facebook owns WhatsApp*. Retrieved from https://spreadprivacy.com/facebook-whatsapp/

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

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a Web site. *Industrial Management & Data Systems, 106*(5), 601–620. doi:10.1108/02635570610666403

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research, 18*(3), 382–388. doi:10.1177/002224378101800313

Garbarino, E., & Johnson, M. S. (1999). The different roles of satisfaction, trust, and commitment in customer relationships. *Journal of Marketing, 63*(2), 70–87. doi:10.1177/002224299906300205

Gefen, D., & Straub, D. W. (2004). Consumer trust in B2C e-Commerce and the importance of social presence: Experiments in e-products and e-services. *Omega, 32*(6), 407–424. doi:10.1016/j.omega.2004.01.006

Gupta, H. (2019). Is Facebook really concerned about privacy? *Columbia Journalism Review*. Retrieved from https://www.cjr.org/tow_center_reports/facebook-merges-encrypted-messages.php/

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). *Multivariate data analysis* (7th ed.). Upper Saddle River, NJ: Pearson.

Hammick, J. K., & Ju, I. (2018). Facebook fan page: The effect of perceived socialness in consumer–brand communication. *Journal of Marketing Communications, 24*(7), 686–702. doi:10.1080/13527266.2016.1205119

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

Hartono, E., Holsapple, C. W., Kim, K. Y., Na, K. S., & Simpson, J. T. (2014). Measuring perceived security in B2C electronic commerce website usage: A respecification and validation. *Decision Support Systems, 62*, 11–21. doi:10.1016/j.dss.2014.02.006

Heirman, W., Walrave, M., Ponnet, K., & Gool, E. V. (2013). Predicting adolescents' willingness to disclose personal information to a commercial website: Testing the applicability of a trust-based model. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 7*(3). doi:10.5817/CP2013-3-3

Hong, I. B., & Cha, H. S. (2013). The mediating role of consumer trust in an online merchant in predicting purchase intention. *International Journal of Information Management, 33*(6), 927–939. doi:10.1016/j.ijinfomgt.2013.08.007

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management, 1*(1), 45–71. doi:10.1023/A:1019104520776

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

Karapanos, E., Teixeira, P., & Gouveia, R. (2016). Need fulfillment and experiences on social media: A case on Facebook and WhatsApp. *Computers in Human Behavior, 55*, 888–897. doi:10.1016/j.chb.2015.10.015

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

Kelly, L., Kerr, G., & Drennan, J. (2017). Privacy concerns on social networking sites: A longitudinal study. *Journal of Marketing Management, 33*(17/18), 1465–1489. doi:10.1080/0267257X.2017.1400994

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544–564. doi:10.1016/j.dss.2007.07.001

Koops, B. J., Newell, B. C., Timan, T., Škorvánek, I., Chokrevski, T., & Galič, M. (2016). A typology of privacy (SSRN Scholarly Paper ID 2754043). *Social Science Research Network*. Retrieved from https://papers.ssrn.com/abstract=2754043

Korkmaz, S., Goksuluk, D., & Zararsiz, G. (2014). MVN: An R package for assessing multivariate normality. *The R Journal, 6*(2), 151–162.

Liu, Z., Min, Q., Zhai, Q., & Smyth, R. (2016). Self-disclosure in Chinese micro-blogging: A social exchange theory perspective. *Information & Management, 53*(1), 53–63. doi:10.1016/j.im.2015.08.006

Lu, B., Fan, W., & Zhou, M. (2016). Social presence, trust, and social commerce purchase intention: An empirical research. *Computers in Human Behavior, 56*, 225–237. doi:10.1016/j.chb.2015.11.057

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

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication, 9*(4), JCMC942. doi:10.1111/j.1083-6101.2004.tb00292.x

Nouwens, M., Griggio, C. F., & Mackay, W. E. (2017). "WhatsApp is for family; Messenger is for friends": Communication places in app ecosystems. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems,* 727–735. doi:10.1145/3025453.3025484

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany: State University of New York Press.

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the UK who use online communities. *European Journal of Information Systems, 19*(2), 181–195. doi:10.1057/ejis.2010.15

Ranganathan, C., & Ganapathy, S. (2002). Key dimensions of business-to-consumer web sites. *Information & Management, 39*(6), 457–465. doi:10.1016/S0378-7206(01)00112-4

Reeves, B., & Nass, C. I. (1996). *The media equation: How people treat computers, television, and new media like real people and places*. Cambridge, UK: Cambridge University Press.

Riquelme, I. P., & Román, S. (2014). Is the influence of privacy and security on online trust the same for all type of consumers? *Electronic Markets, 24*(2), 135–149. doi:10.1007/s12525-013-0145-3

Roloff, M. E. (1981). *Interpersonal communication: The social exchange approach.* Beverly Hills, CA: SAGE.

Rosseel, Y. (2012). lavaan: An R package for structural equation modeling. *Journal of Statistical Software, 48*(2), 1–36. doi:10.18637/jss.v048.i02

Sah, Y. J., & Peng, W. (2015). Effects of visual and linguistic anthropomorphic cues on social perception, self-awareness, and information disclosure in a health website. *Computers in Human Behavior, 45*, 392–401. doi:10.1016/j.chb.2014.12.055

Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing, 16*(3), 2–16. doi:10.1002/dir.10033

Seeger, A. M., & Heinzl, A. (2018). Human versus machine: Contingency factors of anthropomorphism as a trust-inducing design strategy for conversational agents. In F. D. Davis, R. Riedl, J. vom Brocke, P. M. Léger, & A. B. Randolph (Eds.), *Information systems and neuroscience* (pp. 129–139). Cham, Switzerland: Springer.

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

Singh, N., & Sinha, N. (2020). How perceived trust mediates merchant's intention to use a mobile wallet technology. *Journal of Retailing and Consumer Services, 52*. doi:10.1016/j.jretconser.2019.101894

Steenkamp, J. E. M., & Baumgartner, H. (1998). Assessing Measurement invariance in cross-national consumer research. *Journal of Consumer Research*, *25*(1), 78–107. doi:10.1086/209528

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

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

Teo, T., Lee, C. B., Chai, C. S., & Wong, S. L. (2009). Assessing the intention to use technology among pre-service teachers in Singapore and Malaysia: A multigroup invariance analysis of the technology acceptance model (TAM). *Computers & Education, 53*(3), 1000–1009. doi:10.1016/j.compedu.2009.05.017

Van den Broeck, E., Zarouali, B., & Poels, K. (2019). Chatbot advertising effectiveness: When does the message get through? *Computers in Human Behavior, 98*, 150–157. doi:10.1016/j.chb.2019.04.009

Vanian, J. (2018). Facebook is the least trusted major tech company when it comes to safeguarding personal data, poll finds. *Fortune*. Retrieved from https://fortune.com/2018/11/08/mark-zuckerberg-facebook-reputation/

Waldman, A. E. (2016). Privacy, sharing, and trust: The Facebook study. *Case Western Reserve Law Review, 67*(1), 193–234.

Walrave, M., Utz, S., Schouten, A., & Heirman, W. (2016). Editorial: The state of online self-disclosure in an era of commodified privacy. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(1). doi:10.5817/CP2016-1-1

Walsh, G., Beatty, S. E., & Shiu, E. M. K. (2009). The customer-based corporate reputation scale: Replication and short form. *Journal of Business Research, 62*(10), 924–930. doi:10.1016/j.jbusres.2007.11.018

Wang, H., Lee, M. K. O., & Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM, 41*(3), 63–70. doi:10.1145/272287.272299

Wang, M. Y., Zhang, P. Z., Zhou, C. Y., & Lai, N. Y. (2019). Effect of emotion, expectation, and privacy on purchase intention in WeChat health product consumption: the mediating role of trust. *International Journal of Environmental Research and Public Health, 16*(20), 3861. doi:10.3390/ijerph16203861

Waterloo, S. F., Baumgartner, S. E., Peter, J., & Valkenburg, P. M. (2018). Norms of online expressions of emotion: Comparing Facebook, Twitter, Instagram, and WhatsApp. *New Media & Society, 20*(5), 1813–1831. doi:10.1177/1461444817707349

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

Zarouali, B., Van den Broeck, E., Walrave, M., & Poels, K. (2018). Predicting consumer responses to a chatbot on Facebook. *Cyberpsychology, Behavior, and Social Networking, 21*(8), 491–497. doi:10.1089/cyber.2017.0518

Zboja, J. J., & Voorhees, C. M. (2006). The impact of brand trust and satisfaction on retailer repurchase intentions. *Journal of Services Marketing, 20*(6), 381–390. doi:10.1108/08876040610691275

Appendix

The fictitious examples we showed the respondents.

GROUP 1: WhatsApp

GROUP 2: Facebook Messenger