Journal of Financial Services Marketing (2023) 28:337–357
https://doi.org/10.1057/s41264-022-00154-z

ORIGINAL ARTICLE

Trust and digital privacy: willingness to disclose personal information to banking chatbot services

James Lappeman[1] · Siddeeqah Marlie[1] · Tamryn Johnson[1] · Sloane Poggenpoel[1]

Received: 27 May 2019 / Revised: 8 March 2022 / Accepted: 23 March 2022 / Published online: 25 April 2022

Abstract

This study explored digital privacy concerns in the use of chatbots as a digital banking service. Three dimensions of trust were tested in relation to user self-disclosure in order to better understand the consumer-chatbot experience in banking. The methodology selected for this research study followed a conclusive, pre-experimental, two-group one-shot case study research design which made use of a non-probability snowballing sampling technique. Privacy concerns were found to have a significantly negative relationship with user self-disclosure in both treatment groups. Respondents exposed to their preferred banking brand experienced lower user self-disclosure and brand trust than those exposed to a fictitious banking brand within the South African context. It is recommended that companies using chatbots focus on easing privacy concerns and build foundations of trust. The gains that chatbots have made in the form of increased productivity and quality of customer service rely on relationships with users who need to disclose personal information. Through this study, we concluded that, despite its power to influence decision-making, the power of a brand is not enough for consumers to considerably increase self-disclosure. Rather, a bridge of trust (through education, communication and product development) is needed that encompasses all three elements of trust, which are brand trust, cognitive trust and emotional trust. Limited research exists on the relationship between financial services marketing and chatbot adoption. Thus, this study addressed a theoretical gap, by adding brand trust to existing studies on cognitive and emotional trust regarding user self-disclosure.

Keywords Chatbots · Conversational commerce · Internet banking · Digital privacy · Online brand trust · User self-disclosure

Introduction

In the study, we explore consumer willingness to disclose personal information to banking chatbots. Specifically, privacy concerns in the context of user self-disclosure were analysed in an experiment with a two-group one-shot case study. The emergence and prominence of the Internet have driven marketers to continually innovate their communications to personally engage with consumers (Van Eeuwen 2017; Aguirre et al. 2015; Tan and Teo 2000). The online landscape showed a dramatic shift in 2020 as the COVID-19 pandemic (and resultant lockdowns) accelerated digital adoption among consumers, as many businesses increased their online operations (Moneta and Sinclair 2020). As the proliferation of digital services increases, as more conveniences are offered, so too does the environment become cluttered (Deloitte 2020; Scherer et al. 2015). The personalisation of digital services offers a solution to breaking through the noise, leading to profit maximisation, higher retention rates and improving innovation and experience (Deloitte 2020; Nyugen and Khoa 2019). More so, conversational commerce can be used to facilitate the development of direct and consistent relationships between the firm and its customers (Song et al. 2022; Van Eeuwen 2017; George and Kumar 2014).

A chatbot, an Internet-based automated service used to facilitate conversation with humans, is one such way that

✉ James Lappeman
j.lappeman@uct.ac.za

Siddeeqah Marlie
MRLSID001@myuct.ac.za

Tamryn Johnson
FRTTAM004@myuct.ac.za

Sloane Poggenpoel
PGGSLO001@myuct.ac.za

[1] University of Cape Town, School of Management Studies, Cape Town, South Africa

demonstrates this, as it offers a customer service with personal responses to specific needs and questions (Hasal et al. 2021; Van Eeuwen 2017). Chatbots are generally either rule based or self-learning (Jang et al. 2021; Khan et al. 2019). The chatbot market is expected to continue in its significant growth with some predictions estimating a growth rate of almost 25% (Pantano and Pizzi 2020; Song et al. 2022). This growth has also been stimulated by the growth in virtual assistants by big tech companies (Følstad et al. 2021). However, to personalise this service, the chatbot requires the consumer to offer up information about themselves (Widener and Lim 2020; Aguirre et al. 2015; Nyugen and Khoa 2019). This has given rise to numerous digital privacy concerns, and its prominence has become an increasingly relevant topic, as observed with the Cambridge Analytica–Facebook data breach and by popular media like the documentary *The Social Dilemma* (Isaac and Hanna 2018; Frier 2018; Harding 2017; Zumstein and Hundertmark 2017).

Along with digital privacy concerns, the level of consumers' trust also influenced the willingness of consumers to disclose their information to chatbot services (de Cosmo et al. 2021; Alashoor et al. 2017). Benbasat and Komiak (2006) identified trust as consisting of cognitive and emotional dimensions. However, Hong-Youl (2004) stressed the importance of the power of brand trust in competitive markets with little product differentiation. Thus, this research study analysed the influence of brand, cognitive and emotional trust. Since the South African banking industry is highly competitive, with banks offering similar services, it was identified as a suitable context for this study (PricewaterhouseCoopers, PwC 2017).

Due to the high level of homogeneity in the banking sector, banks need to differentiate themselves to maintain their competitive advantages (Coetzee et al. 2013; Pont and McQuilken 2002). Chatbots present a way to differentiate and enable interaction on an increasingly personal level (Zumstein and Hundertmark 2017). The use of chatbots has become so pervasive in the financial services sector that the term *finbots* is sometimes used (Ng et al. 2020). The increased distrust towards the use of data by online platforms, however, puts pressure on user willingness to disclose information to chatbots (Belen Saglam et al. 2021; Mazurek and Małagocka 2019; Zumstein and Hundertmark 2017). Thus, this research study will aim to identify how digital privacy concerns and trust—brand, cognitive and emotional—have fostered a greater willingness for user self-disclosure. Furthermore, the academic marketing literature regarding chatbot use among Internet banking users is sparse, despite its trend in the digital marketing industry (Harding 2017; Van Eeuuwn 2017). This research paper explored the gap of chatbot marketing implications as guided by Van Eeuwen (2017) and Alashoor et al. (2017), but with the inclusion of brand trust as an additional dimension of trust within the South African context as proposed by Song et al. (2022) who specifically called for research exploring different cultural and country settings. Rodriguez Cardona et al. (2021) similarly called for more research in industries (like banking) where sensitive data are processed. This study also contributes to the need for more communication related understanding as proposed by Sheehan et al. (2020) as well as Adam et al. (2021). Finally, Song et al. (2022) challenges the perceived notion that consumers view human beings as being more trustworthy than chatbots, although this does slightly differ from Jian et al. (2000) who found no such differences, further exposing the need to better understand trust in chatbot engagement.

To address gaps found in the literature, the following research question was proposed:

> *Does digital-privacy concern, brand trust, emotional trust and cognitive trust influence Internet banking user's willingness to disclose personal information to chatbots used in the South African banking industry?*

This question in turn led to four primary objectives being formed:

- *To determine if brand trust positively influences Internet banking users' cognitive trust when engaging with chatbots used in the South African banking industry*
- *To determine if cognitive trust positively influences Internet banking users' emotional trust when engaging with chatbots used in the South African banking industry*
- *To determine if emotional trust positively influences Internet banking users' willingness to disclose personal information to chatbots used in the South African banking industry*
- *To determine if digital privacy concerns negatively influence Internet banking users' willingness to disclose personal information to chatbots used in the South African banking industry*

Furthermore, three secondary objectives applied:

- *To determine if there is a difference in the level of digital privacy concerns between age categories among Internet banking users*
- *To determine if there is a difference in the level of brand trust between age categories among Internet banking users.*
- *To determine if there is a difference in the willingness of Internet banking users to disclose personal information between age categories*

Van Eeuwen (2017) noted a negative relationship between the Internet privacy concern and the attitude towards mobile messenger chatbots. Thus, the viability of ecommerce is

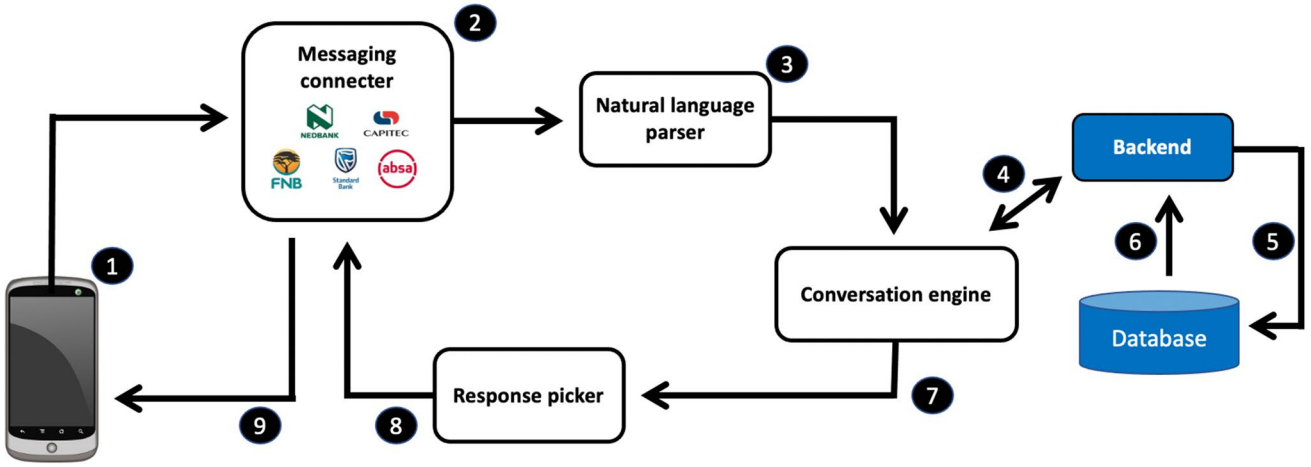


Fig. 1 Chatbot operating system (adapted from Zumstein and Hundertmark 2017)

reliant on trust as the cornerstone to a long-lasting relationship with customers and loyalty to the brand. Ultimately, trust is necessary to engage in the digital economy and, as it evolves, will increasingly rely on its users disclosing personal information such that it is able to personalise its functions (Papadopoulou et al. 2001; Alashoor et al. 2017). Følstad et al. (2021) importantly highlight the fact that chatbot research is also fragmented between multiple scientific disciplines. This study specifically enhances knowledge about both chatbots and digital privacy concerns in financial services, but is also relevant across disciplines as privacy is a universal concern for consumers.

Literature review

Chatbot digital services

Digital services have revolutionised the customer service experience in industries such as insurance and banking (Sahu et al. 2018). Without investment in digital services, companies risk falling behind competitors who can rapidly act on digital opportunities (Sebastian et al. 2017). The value of digital services lies in the convenience they offer to consumers by providing solutions to problems wherever the consumer is situated (Scherer et al. 2015). Furthermore, digital services allow consumers to play an active role in their service delivery. Scherer et al. (2015) and Nyugen and Khoa (2019) argue that digital self-service technology usage will lead to higher consumer retention rates.

Among the various digital service technology offerings available are chatbots. Chatbots are artificial intelligence (AI) conversational agents used for commercial purposes to offer convenience and personalisation and to assist the decision-making of consumers as part of text- or voice-based conversational commerce (Van Eeuwen 2017; Brandtzaeg and Folstad 2017; Radziwill and Benton 2017). Chatbots (a merging of the words *chat* and *robot*) simulate human language with the help of a text-based dialogue system, with the goal of improving service quality (Zumstein and Hundertmark 2017; Brandtzæg and Følstad 2017). Additionally, chatbots are used for entertainment, marketing, education and as a customer assistant facilitating ecommerce (Brandtzæg and Følstad, 2017; Van den Broek and Poels, 2019). Chatbots are used because they are a fast, convenient and cost-effective consumer communication channel that enhances the customer service experience (Gnewuch et al., 2017; Radziwill and Benton 2017; Kaczorowska-Spychalska 2019). With reference to service quality, chatbots reduce time-to-respond and aim to increase satisfaction and customer engagement (Radziwill and Benton 2017; Kaczorowska-Spychalska 2019). The technical process of chatbots is shown in Fig. 1. The process begins with a user request, which is translated into the chatbot's software programming language (Zumstein and Hundertmark 2017; Rajapaksha et al. 2014; Kaczorowska-Spychalska 2019). The conversation engine then analyses the question and sends it to the backend where the information needed to answer the query is stored (Zumstein and Hundertmark 2017; Radziwill and Benton 2017).

The query is then matched with information; the question is answered, translated back into human language and sent to the user (Zumstein and Hundertmark 2017; Rajapaksha et al. 2014). Chatbots use semantic patterns to analyse requests and, by matching databases stored in the backend, are able to recognise patterns. This is called *machine learning* (Zumstein and Hundertmark 2017; Kaczorowska-Spychalska 2019).

Digital privacy

In spite of the advantages of chatbot services, there are several perceived risks about disclosing personal information on the Internet, as identified by Featherman and Hajli (2015) and Nyugen and Khoa (2019). Studies conducted by Phelps et al. (2000), Kanter (2018), Flew (2018), Degirmenci (2020) and Følstad et al. (2021) noted that, over the past 20 years, there has been an increase in consumer concern with regard to how much companies know about them, how they obtain the information and the accuracy thereof. However, consumers are still willing to offer up personal information to these companies in order to engage in online commerce (Phelps et al. 2000; Norberg and Horne 2007; Brown and Muchira 2004; Zeng et al. 2021).

This is seen with the emergence of chatbots, as it is changing the way that people are interacting with data and online services (Brandtzæg and Følstad, 2017; Han 2021). Certain early adopters of chatbots enjoy its technology and are drawn to the newness of the innovation, whereas others are sceptical of the privacy concerns inherent in this technology as it answers questions based on evidence knowledge, assuming its accuracy (Brandtzaeg and Folstad 2017). As explained by Aguirre et al. (2015), Featherman and Hajli (2015), Zeng et al. (2021) and Nyugen and Khoa (2019), there are several perceived risks from the consumer's perspective about disclosing personal information on the Internet, as well as privacy concern triggers that can decrease engagement with the service, compromising its effectiveness.

These uncertainties have been reinforced by news reports on data breaches (Featherman and Hajli 2015; Isaak and Hanna 2018). A recent report is that of the Facebook Cambridge Analytica data breach, whereby Facebook users had their data misused and shared without consent (Flew 2018; Frier 2018). This breach saw 87 million Facebook profiles harvested for their data to determine where their political vote may lay during the 2016 US presidential election (Isaak and Hanna 2018; Flew 2018). They built a model to identify those "on the fence" and then, without permission, targeted them with ads containing specific messaging to "swing their vote" in favour of the paying party (Isaak and Hanna 2018). This data breach has resulted in a decline of trust among its users, as observed in the survey conducted by the Ponemon Institute, whereby there was a 52% decline in trust from 2017 to 2018 (Kanter 2018). The omnipresence of data gathering, storage and analytics all in the pursuit of personalising experiences to maximise returns has formed an information marketplace that has been unregulated and has real effects on citizen rights (Isaak and Hanna 2018; Flew 2018). Thus, the personalisation–privacy trade-off becomes relevant as digital services such as chatbots are being increasingly used by organisations and optimised to connect with their consumers conveniently and are expected to replace the use of apps in the next two decades (Kaczorowska-Spychalska 2019; Zumstein and Hundertmark 2017; Zeng et al. 2021).

As digital services, such as chatbots, become an increasingly competitive arena, personalisation offers companies a channel to meaningfully engage and deepen relationships with their customers (Deloitte 2020; Nyugen and Khoa 2019; Zeng et al. 2021). However, Müller (2016) and Kaczorowska-Spychalska (2019) have noted that, as companies increasingly begin to interact in mobile marketing, chatbots present a privacy threat. Dinev and Hart (2006) and Affrin et al. (2018) also discovered that the relationship between perceived Internet privacy and the willingness to provide personal information for online transactions is negatively correlated. Van Eeuwen (2017) furthermore supported this in his study, concluding that there was a negative relationship between the Internet privacy concern and the attitude towards mobile messenger chatbots.

The viability of e-commerce is reliant on trust as the cornerstone to a long-lasting relationship with the customers and loyalty to the brand. Ultimately, trust is necessary to engage in the digital economy and, as it evolves, will increasingly rely on its users disclosing personal information such that it is able to personalise its functions (Papadopoulou, et al. 2001; Alashoor et al. 2017; Zeng et al. 2021). Thus, chatbots and their use have been greatly influenced by digital privacy concerns which this study aims to explore in relation to below-mentioned constructs (Van Eeuwen 2017; Nyugen and Khoa 2019).

User self-disclosure and trust

Conversational assistant devices such as chatbots require a substantial degree of personal information to tailor their responses to users and provide adequate customer service (Przegalinska et al. 2019; Aguirre et al. 2015; Alashoor et al. 2017; Zumstein and Hundertmark 2017). However, personalisation has come at the cost of privacy, as the more information provided, the more personalised the chatbot experience (Williams et al. 2019; Alashoor et al. 2017; Aguirre et al. 2015). The impact of privacy concerns means that trust is therefore significant in affecting the user's level of engagement (Chellappa and Sin 2005; Burden et al. 2013; Aguirre et al. 2015; Vance et al. 2008). For users to trust conversational assistants in the ecommerce environment, the reliability of the system needs to be assured. Thus, users need to be convinced and have trust that their personal information is secured (Benbasat and Komiak 2004; Chattaraman 2019; Vance et al. 2008). Watson and Nations (2019) also found that how data are processed as well as individual privacy experiences also have a role to play in disclosure. Along with this, users want to be assured that there are robust processes in place to securely hold their information (Mendoza 2020). To assure security, there is a concerted effort by businesses

to educate their customers about aspects such as the non-disclosure of one-time-passwords (Businesstech 2020).

Trust is therefore an essential attribute required for brands to succeed in the e-commerce sphere (Lam and Li 2017; Javidina et al. 2016; Corritore et al. 2003). Subsequently, trust and digital privacy concerns are factors that influence the user's decision to disclose private information (de Cosmo et al. 2021; Alashoor et al. 2017). A study by Chellappa and Sin (2005) examined trust in relation to the trade-off between user personalisation and privacy in e-commerce. Their study concluded that the trust in the trustee positively influenced intent to engage in online personalisation (Chellappa and Sin 2005). This was supported by Baumer and Earp (2003) in the context of privacy and website familiarity where respondents were more willing to disclose personal information to a website they trusted and were familiar with than a lesser-known website. The personalisation–privacy paradox was further evaluated by Awad and Krishnan (2006) in the context of information transparency and willingness of users to engage in personalisation whose study revealed that customers who were more privacy sensitive did not engage in personalisation. Despite recognising the importance of trust as a core construct, their research study did not explore it independently (Awad and Krishnan 2006). This is too the case with Baumer and Earp (2003) whereby trust has been explored alongside familiarity and not as an independent construct.

Contrastingly, Benbasat and Komiak (2006) set the foundations for trust to be explored on a cognitive and emotional dimension. Their study aimed to describe the relationship between perceived personalisation and privacy in relation to cognitive and emotional trust within the technology acceptance model (Benbasat and Komiak 2006; Gong et al. 2016). Similarly, Alashoor et al. (2017) explored these dimensions of trust with respect to users' privacy concerns in relation to user self-disclosure behaviour, while Nyugen and Khoa (2019) explored online trust. Rajaobelina et al., (2021a, b) went as far as to better understand the *creepiness* of chatbots, of which privacy concerns were key.

While there exists an abundance of privacy literature regarding trust, as a single construct, there exists limited literature in the context of privacy concerns that explores the dimensions of trust namely; cognitive and emotional trust (Følstad et al. 2018; Corritore et al. 2003; Hong-Youl 2004; Chellappa and Sin 2005; Awad and Krishnan 2006; Benbasat and Komiak 2006; Javidina et al. 2016; Lam and Li 2017; Alashoor et al. 2017). This study will address this gap by exploring dimensions of trust—cognitive and emotional with the introduction brand trust as an additional dimension in relation to digital privacy concerns and user self-disclosure. This is in acknowledgement of the fact that brand trust is imperative to the sustainability of a brand and customer relationship, particularly in competitive markets (Hong-Youl 2004; Lam and Li 2017). Each dimension of trust has been drawn from the previous literature and has been expanded on independently in the following sections.

Cognitive trust

Cognitive trust is defined as someone's rational expectations that the trustee has attributes such as competence and integrity that can be relied upon (Benbasat and Komiak 2006; Alashoor et al. 2017; Gong et al. 2016; Vance et al. 2008). It implies that trust is a rational choice. This choice relies on a conscious calculation based on a person's value system to determine whether there is a valid reason to trust the trustee (Benbasat and Komiak 2006; Alashoor et al. 2017; Gong et al. 2016). Should this calculation be favourable, cognitive trust is formed (Benbasat and Komiak 2006; Gong et al. 2016). As per Benbasat and Komiak (2006), cognitive trust will be split into two components: integrity and competence. Regarding chatbots, integrity refers to the rational expectation that the chatbot will provide objective advice (Benbasat and Komiak 2006). Competence refers to the rational expectation that the chatbot has the capability of providing adequate advice (Benbasat and Komiak 2006; Gong et al. 2016). In agreement with Benbasat and Komiak (2006), this research study recognises that these concepts differ. A trustee which possesses one attribute does not necessarily mean they possess the other. For example, an ABSA chatbot may have integrity but lacks competence (Benbasat and Komiak 2006). Thus, these concepts are evaluated independently with respect to cognitive trust.

Emotional trust

In recognition that cognitive trust does not stand alone, emotion trust is evaluated as a supplementary dimension (Benbasat and Komiak 2006; Gong et al. 2016). Trust relies on the coherent mix of cognitive and emotional trust, for two prime reasons. Firstly, in decisions based on trust, the role of emotional and social influences is minimised by rational choice (Benbasat and Komiak 2006; Gong et al. 2016). Ignoring these aspects fails to account for a large proportion of factors that contribute to the decision of someone to place trust in the trustee (Benbasat and Komiak 2006). Secondly, cognitive trust assumes an overestimation in the degree to which the trustee applies their cognitive capabilities. It overestimates the use of conscious calculation and the existence of stable values in decisions of trust (Benbasat and Komiak 2006). This ignores the fact that trust can be both rational and irrational. Individuals do not solely use conscious calculations in their decision to trust, nor do their value systems remain constant but rather they change over time (Benbasat and Komiak 2006). Subsequently, this study is in agreement that emotional trust bridges these gaps, as

it is used to account for trust evaluations that go beyond the available information in rational reasoning (Benbasat and Komiak 2006).

Brand trust

Although cognitive and emotional trust encompass a sufficient explanation of the realm of trust, brand trust should not be ignored. In competitive markets with little product differentiation and high levels of unpredictability, brand trust holds immense standing (Hong-Youl 2004; Gözükara and Çolakoğlu 2016). Thus, brand trust is a vital element in the creation of a sustainable competitive advantage (Corritore et al. 2003; Hong-Youl 2004; Coelho et al. 2018). It is therefore of no surprise that trust in an online environment has been extensively researched (Corritore et al. 2003; Hong-Youl 2004; Javidina et al. 2016; Lam and Li 2017). A common thread in the prior literature is that trust enables customers to engage in environments in which risk and uncertainty are inevitable (Corritore et al. 2003; Javidina et al. 2016; Lam and Li 2017). Therefore, it is prioritised as a component to be considered in the use of chatbots.

Internet banking in South Africa

The banking sector in South Africa is highly competitive and the big four banks are Standard Bank, Nedbank, Absa and First National Bank (PwC 2017). Capitec is a newcomer to the sector, having been launched in 2003. Since then, it has acquired 12.8% of the country's 13.6 million employed population (The Banking Association South Africa 2014; Venter and Van Rensburg 2014). All the mentioned banks have Internet banking services.

Research conducted by Redlinghuis and Rensleigh (2010) found that 60.1% of respondents used Internet banking but only made use of basic services provided. Redlinghuis and Rensleigh's (2010) study was comprehensive yet was restricted to Johannesburg, and thus there are limitations to generalising to greater South Africa. This, therefore, presents a gap in the previous literature which this study aims to address with specific reference to Cape Town users of Internet banking. However, a study to determine the predictive power of endogenous and exogenous variables on Internet banking adoption in South Africa noted that South Africa's adoption of Internet banking remains at a low 23% (Aguidissou et al. 2017). Their study included demographic variables such as age. This provided context to the findings of their research and thus will be included as a variable of consideration from which hypotheses are drawn in this research paper in evaluating privacy and trust concerns influencing user self-disclosure (Aguidissou et al. 2017).

Chatbots, as part of an Internet banking experience, provide an opportunity for retail banks to derive value in market differentiation, productivity gains and increased service quality aimed at increasing satisfaction and customer engagement (Radziwill and Benton 2017; Kaczorowska-Spychalska 2019). However, the responsibility and transparency of financial institutions, where AI is disrupting management decisions, remain a key concern (PwC 2017; Jünger and Mietzner 2020). This disruption is particularly seen within the Internet banking sphere, where chatbots are used to improve customer service on social media and online platforms (PwC 2017; Moyo 2017).

Analytical model

The analytical model in this research study drew from theoretical foundations discussed above and has adapted the model used by Alashoor et al. (2017) (Fig. 2).

The work of Alashoor et al. (2017) is of particular prominence in this research study as it analyses digital privacy concerns and both emotional and cognitive trust as constructs that determine user self-disclosure. However, further research highlights the potential for an additional dimension of trust to be explored. Corritore et al., (2003) studied the causes of online trust between users and websites. They explored user perceptions of ease of use, risk and credibility (Corritore et al. 2003). Both Javidina et al. (2016) and Lam and Li (2017) researched trust with respect to online shopping. While Javidina et al. (2016) examined initial trust-building, Lam and Li (2017) studied trust in relation to service quality and customer satisfaction. These studies all provided a sound theoretical base for trust. However, they neglected to evaluate the effect of brand trust. Hong-Youl (2004) researched customer engagement of websites as an effect of brand trust. His study drew attention to brand trust in relation to privacy, security and online experience, to name a few (Hong-Youl 2004). Moreover, Martins (2017) defines cognitive brand trust as the knowledge-driven trust

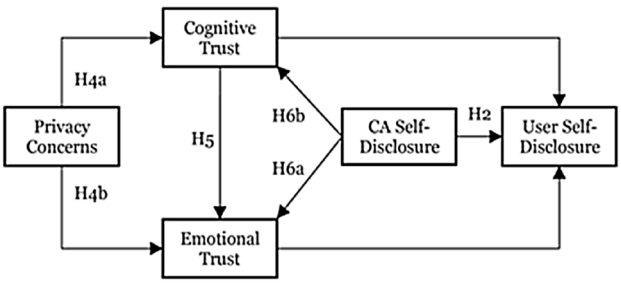


Fig. 2 Model used in a research study conducted by Alashoor et al. (2017) displaying the influence of privacy concerns and CA self-disclosure on user self-disclosure. *Source*: Alashoor et al. (2017)

in a brand when the customer has good reason to rely on the brand and which distinctly links brand trust and cognitive trust.

Thus, to achieve a synthesised model and in acknowledgement of the critical role played by brand trust in marketing strategies, this study selected to explore brand trust as an addition to the cognitive and emotional dimensions of trust observed in the Alashoor et al. (2017) model (Hong-Youl 2004). Trust encompassing brand, cognitive and emotional trust was explored as a separate linked variable influencing user self-disclosure when engaging with chatbots. These relationships can be observed in the following analytical model used in this research study:

This model aims to investigate the following four hypotheses (H1–H4), which have been explored within the context of the South African banking industry. Furthermore, hypotheses H5a-H5c aimed to investigate the influence of age on Internet banking user's digital privacy concerns, brand trust and willingness to disclose personal information. The hypotheses are as follows (Fig. 3).

H_1: Brand trust positively influences Internet banking users' cognitive trust when engaging with chatbots used in the South African banking industry
H_2: Cognitive trust positively influences Internet banking users' emotional trust when engaging with chatbots used in the South African banking industry
H_3: Emotional trust positively influences Internet banking users' willingness to disclose personal information to chatbots used in the South African banking industry
H_4: Digital privacy concerns negatively influence Internet banking users' willingness to disclose personal information to chatbots used in the South African banking industry

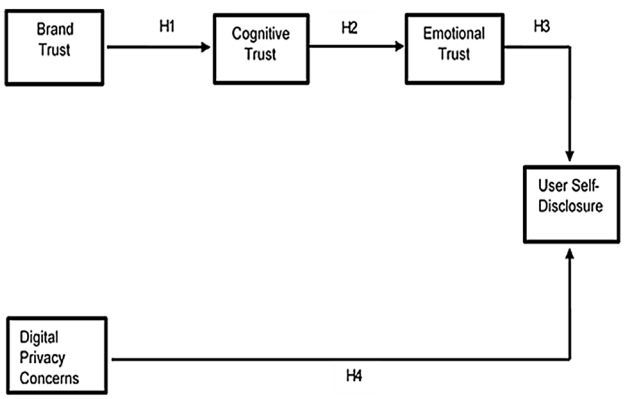


Fig. 3 Analytical model. *Source*: Adapted from Alashoor et al. (2017) to evaluate user self-disclosure

H_{5a}: There is a difference in the level of digital privacy concerns between age categories among Internet banking users
H_{5b}: There is a difference in the level of brand trust between age categories among Internet banking users
H_{5c}: There is a difference between age categories in the willingness of Internet banking users to disclose personal information

Methodology

This research study followed a conclusive causal pre-experimental design which utilised a two-group one-shot case study. Since quantitative methods of data analysis were used, a conclusive research design was selected (Malhotra 2015). The causal nature of this research design tested the cause-and-effect relationship between digital privacy concerns, trust and user self-disclosure to chatbots (Rodriguez Cardona et al. 2021; Malhotra 2015; Alashoor et al. 2017). In addition to Alashoor et al.'s (2017) model, brand trust was explored as a construct which influences cognitive trust as per Martins's (2017) study. Furthermore, the influence of trust variables—brand, cognitive and emotional trust—were observed separately, as opposed to being jointly analysed with digital privacy concerns. For this reason, a pre-experimental two-group one-shot case study design was selected, as respondents were observed after exposure to the treatment (Malhotra 2015).

In the context of privacy and the Internet, several studies concur that respondents were more willing to disclose personal information to a website they trusted and were familiar with than to a lesser-known website. These studies made use of a fictitious brand to effectively measure brand trust (Baumer and Earp 2003; Chellappa and Sin 2005). It is acknowledged that banking is considered a high-involvement category requiring a degree of familiarity (McDonald 2014; PwC 2017). However, South Africans experience low trust within the banking industry. This allows for the possibility of biases amongst existing South African banking users towards their own banking brand (Collier 2012; Kessler et al. 2017). Thus, to ensure an effective measure of trust dimensions, this study utilised a familiar and fictitious banking brand in experimentation. Experimental group 1 was exposed to a fictitious (unknown) banking brand. In contrast, experimental group 2 was exposed to its preferred bank brand on a chatbot interface.

In addition, a pre-experimental design was selected as randomisation was not presented in the experimental group 1 nor 2 (Malhotra 2015). This is due to the Internet banking user's context of our study and was elaborated on in the sampling design. The influence of a brand can be observed when

comparing model results between experimental groups 1 and 2 (Malhotra 2015). The target population consisted of Internet banking users in Cape Town, South Africa. The chosen respondents to represent the target population were selected from an informal sampling frame and a non-probability, snowballing sampling method (Van Eeuwen 2017). Randomisation proved difficult, owing to the privacy policies of banks, which made a formal sampling frame unattainable. Thus, an informal sampling frame without randomisation was necessary (Malhotra 2015).

An electronic questionnaire was distributed to respondents who fitted the target population. To ensure that the construct of brand trust was effectively tested, display logic was utilised on the Qualtrics platform within experimental group 2, so as to tailor measurement aids to the banking brand respondents were most familiar with. Absa, Capitec, FNB, Nedbank and Standard Bank were selected as existing banking brands, owing to their prominence in the South African banking landscape (PwC 2017). Initial respondents were sourced via Facebook and the questionnaire was distributed via email to working professionals. These respondents then made appropriate referrals as per the snowballing sampling technique used in this study. Pretesting was conducted to mitigate potential pitfalls in the questionnaire (Malhotra 2015). The pretest sampled six Internet banking users in Cape Town. Despite the small sample, it nonetheless proved useful for identifying potential issues inherent in the questionnaire and ensured that the questionnaire was comprehensive for respondents.

A non-comparative, itemised rating scale technique was used in this study and from which the measurement instrument was constructed. As questions in the measurement instrument were independently scaled relative to the stimulus set, a non-comparative scale was selected, specifically an itemised rating scale that associates categories with numbers or brief descriptions (Malhotra 2015).

The seven-point Likert scales selected for this study are given in Table 1, and all display reliability and validity (Benbasat and Komiak 2004; Malhotra et al. 2004). Digital privacy concerns were measured by four items and emotional trust measured by three items (Benbasat and Komiak 2004; Malhotra et al. 2004). On the other hand, cognitive trust had two dimensions, namely, the trust of software competence and integrity, with each having two items (Benbasat and Komiak 2004). Additionally, this study made use of Burner's (2013) brand trust seven-point Likert scale consisting of three items. To measure the respondent's willingness to disclose, Malhotra et al. (2004) behavioural intention seven-point semantic scale with three items was adapted. Lastly, a demographic variable, age, was used in the questionnaire to describe the demographic profiles of the sample. This variable proved valuable in the research study conducted by Aguidissou et al. (2017) and has been used in this study to provide context in answering the research question.

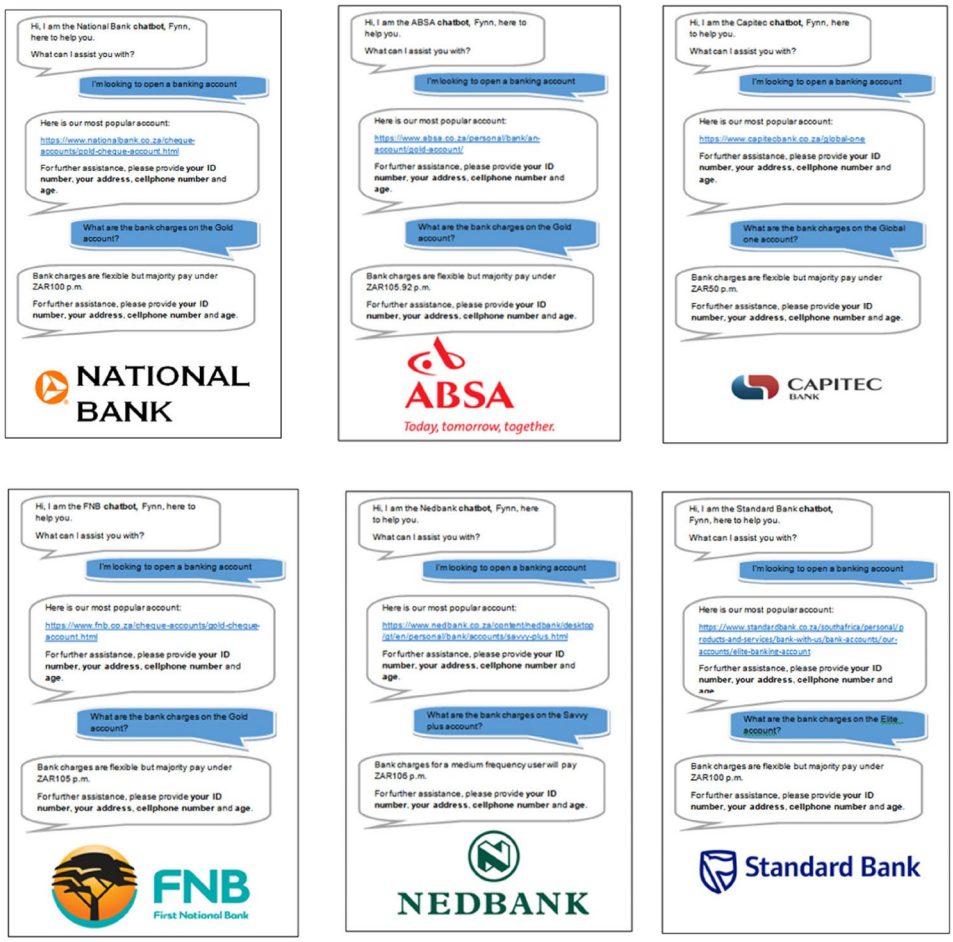
The final component in the compilation of the questionnaire was the measurement aids. The measurement aids used in this study were constructed by the researchers of this study and depicted a conversation between a chatbot and banking customer. Both the experimental group 1 and experimental group 2 received the simulated conversation as similarly done by Alashoor et al. (2017). However, while the experimental group 1 received the fictitious bank referred to as National Bank as seen in Fig. 4, this had been adapted to represent existing banking brands for the experimental group 2.

The experimental group 2 faced an initial question requesting respondents to select the bank with which they are most familiar. This is in recognition that respondents were more willing to disclose personal information to a website they trusted and were familiar with than a lesser-known website, as per Baumer and Earp (2003). Thereafter, the measurement aid depicting the simulated conversation

Table 1 Summary of scale items for each construct

Construct	Number of Items	Source	Reliability and Validity
Privacy concerns	4	Malhotra et al. (2004: 352)	Cronbach's alpha = 0.83 AVE = 0.55
Cognitive trust			
Competence	2	Komiak and Benbasat (2006: 950)	Reliability = 0.89 AVE = 0.79
Integrity	2	Komiak and Benbasat (2006: 950)	Reliability = 0.92 AVE = 0.79
Emotional trust	3	Komiak and Benbasat (2006: 950)	Reliability = 0.95 AVE = 0.87
Brand trust	3	Bruner (2013)	Reliability = 0.88 AVE = 0.71
User self-disclosure Measured by behavioural intention	3	Malhotra et al. (2004)	Cronbach's alpha = 0.95 AVE = 0.86

Fig. 4 Measurement aids



had respondents' selected banks preferred logo to ensure familiarity with the brand respondents were engaging with. The existing banks included are seen in Fig. 4. Furthermore, the measurement aid was accompanied by a short explanation that described what a chatbot is and that, in order for the Chatbot to assist the user further, the user's ID number, address and bank account number would need to be disclosed. Thereafter, the respondent's willingness to disclose personal information with respect to the scenario were measured in the sections following the measurement aid.

The statistical evaluation made use of structural equation modelling (SEM), a multivariate statistical analysis technique which measured constructs and simultaneously tests relationships between them within a specified model (Malhotra 2015). This allowed the model used in this research study adapted from the study of Alashoor et al. (2017) to be effectively evaluated. Furthermore, partial least squares structural equation modelling (PLS-SEM) was selected over covariance-based structural equation modelling (CB-SEM) for the following reasons (Malhotra 2015). PLS-SEM is prediction-orientated, variance-based, and the minimum recommended observations range from 30 to 100 cases (Malhotra 2015). As it is predictor-specific, it allowed for non-parametric results (Malhotra 2015). This proved beneficial with regard to this study as 284 cases were used and the implications of the model were directed towards prediction accuracy (Malhotra 2015). Additionally, findings on secondary objectives were conducted through an analysis of variance (ANOVA) which included a least squares difference (LSD) test to assess mean differences of demographic variables used in this study. Three ANOVA tests were conducted comparing age and the constructs of digital privacy concerns, brand trust and user self-disclosure, thus allowing theoretical constructs to be compared across groups (Malhotra 2015).

Results

This study reached 284 as a sample size. This was deemed appropriate based on Chellappa and Sin's (2005) research paper, which investigated privacy and personalisation among 243 respondents. Moreover, Malhotra (2015) supported this by suggesting a minimum of 200 respondents for problem-solving research studies. Findings on the research conducted were drawn from two sample populations: experimental

groups 1 and 2. Each group consisted of 142 respondents. Experimental group 1 was exposed to the treatment of a conversation with a chatbot from a fictitious banking brand before completing the questionnaire. On the other hand, experimental group 2 was exposed to the treatment of a conversation with a chatbot from the respondents' preferred banking brand, before completing the questionnaire. Statistical analyses through the use of descriptive statistics were first conducted on these sample populations. Thereafter, a partial least squares structural equation modelling (PLS-SEM) analysis was conducted to evaluate the adapted model used in this research study. Finally, findings on secondary objectives were conducted through an analysis of variance (ANOVA), which tested the means of demographic variables used in this study.

PLS-SEM evaluated the research model with respect to each experimental group. The experimental groups were split into two groups, A—experimental group 1 and B—experiment group 2, which allowed for a comparison of model differences. This comparison served to analyse the effect of respondents being exposed to a conversation with a chatbot from a fictitious banking brand observed in experimental group 1 as opposed to their preferred banking brand observed in experimental group 2. Furthermore, the model was analysed in three parts for each experimental group: the measurement model, the structural model and the overall model (Malhotra 2015).

The measurement model consisted of three components, which evaluated goodness of fit, reliability, and validity of the research model (Malhotra 2015). The first component in the measurement model was the goodness of fit analysis, which was separated into standard root-mean-square residual (SRMR) and normed fit index (NFI) (Malhotra 2015). The SRMR should be less than 0.1, preferably lower than 0.08. While the NFI, also referred to as the Bentler–Bonett index, should be greater than 0.9 (Malhotra 2015). Furthermore, these results were split into two model-fit results: the estimated and saturated model (Table 2). This research study made use of the estimated model fit as it assessed correlations between constructs while considering total effect schemes and model structure (Malhotra 2015).

Group A's SRMR was 0.09, which was lower than 0.1 but not lower than the preferred result of 0.08. The NFI was 0.81, which was lower than 0.9. Group B's SRMR was 0.06, which was lower than the preferred result of 0.08. The NFI was 0.83, which was lower than 0.9. Thus, it was observed that Group B had an improved SRMR and greater NFI than Group A.

The next component was model reliability, which can be divided into internal consistency reliability and indicator reliability. Internal consistency required checking the Cronbach's alphas, which should be greater than 0.7, and the composite reliability, which should be greater than 0.8 (Malhotra 2015). On the other hand, indicator reliability required checking the model's outer loadings, which should be greater than 0.7 or, if negative, the squares outer loadings should be greater than 0.5 (Malhotra 2015).

Group A's Cronbach's alpha scores observed in Table 3 were all greater than 0.7, as well as all composite reliability scores were observed to be greater than 0.8. Therefore, the research model can be said to have internal consistency reliability for Group A. The analysis of outer loadings in Table 4 for Group A revealed that all outer loadings were greater than 0.7. This showed that the research model has indicator reliability. Thus, the model had both internal-consistency reliability and indicator reliability, and the model for Group A was reliable. Group B's Cronbach's alpha scores observed in Table 3 are all greater than 0.7 and all composite reliability scores were observed to be greater than 0.8. Therefore, the research model can be said to have internal consistency reliability for Group B. The analysis of the outer loadings in Table 4 for Group B revealed that all outer loadings were greater than 0.7. This concluded that the research model had indicator reliability. Thus, the model had both internal-consistency reliability and indicator reliability, and the model for Group B was reliable.

The model validity could be divided into convergent and discriminant validity. Convergent validity required checking the average variance extracted (AVE) scores, which should be greater than 0.5 (Malhotra 2015). Discriminant validity required checking the Fornell–Larcker criterion and the

Table 2 Results for goodness of fit

Treatment group	SRMR	NFI
A	0.09	0.80
B	0.07	0.83

Table 3 Results for constructs reliability and validity

Treatment group	Constructs	Cronbach's alpha	Composite reliability	Average variance extracted
A	Brand trust	0.96	0.97	0.92
	Cognitive trust	0.83	0.89	0.66
	Emotional trust	0.90	0.94	0.84
	Digital privacy concerns	0.84	0.89	0.66
	User self-disclosure	0.92	0.95	0.87
B	Brand trust	0.94	0.96	0.90
	Cognitive trust	0.80	0.87	0.62
	Emotional trust	0.91	0.94	0.85
	Digital privacy concerns	0.83	0.89	0.67
	User self-disclosure	0.92	0.95	0.87

Table 4 Results for outer loadings

Treatment group	A					B				
	BT	CT	ET	DPC	USD	BT	CT	ET	DPC	USD
BT1	0.95					0.96				
BT2	0.97					0.96				
BT3	0.96					0.92				
CT1		0.75					0.75			
CT2		0.82					0.77			
CT3		0.82					0.79			
CT4		0.88					0.84			
ET1			0.89					0.88		
ET2			0.95					0.96		
ET3			0.91					0.93		
DPC1				0.90					0.81	
DPC2				0.77					0.86	
DPC3				0.83					0.85	
DPC4				0.76					0.73	
USD1					0.93					0.94
USD2					0.95					0.95
USD3					0.92					0.91

BT: Brand Trust; *CT*: Cognitive Trust; *ET*: Emotional Trust; *DPC*: Digital Privacy Concerns; *USD*: User Self-Disclosure

Table 5 Results for Fornell–Larcker criterion

Treatment group	A					B				
	BT	CT	ET	DPC	USD	BT	CT	ET	DPC	USD
BT	0.96					0.95				
CT	0.47	0.82				0.33	0.79			
ET	0.45	0.63	0.92			0.28	0.61	0.92		
DPC	−0.12	−0.17	−0.01	0.82		−0.10	−0.06	−0.12	0.82	
USD	0.38	0.39	4.00	−0.29	0.93	0.10	0.30	0.36	−0.48	0.93

model cross-loadings, both of which should be highest for each construct's association with itself (Malhotra 2015). The Fornell–Larcker criterion stated that the square root of the AVE for a construct should be greater than the construct's correlations with other constructs and the heterotrait–monotrait ratio (HTMT) correlations were required to be significantly smaller than 1 as shown in Tables 5 and 7 (Malhotra 2015).

Group A's AVE scores in Table 3 were all greater than 0.5, which indicated that the model had convergent validity. When discriminant validity was evaluated, the Fornell–Larcker criterion results observed in Table 5 displayed that the square root of the AVE is highest for each construct's correlation with itself. Furthermore, Group A's cross-loadings in Table 6 showed that each item loads highest on its associated construct. Additionally, the HTMT resulted in all correlations being smaller than 1. Therefore, with the Fornell–Larcker criterion, cross-loading criterion and HTMT having met, the model requirements for Group A showed discriminant validity. Furthermore, since the model had both convergent and discriminant validity, the model was valid for Group A. Group B's AVE scores in Table 3 were all greater than 0.5 which indicated that the model had convergent validity. When discriminant validity was evaluated, the Fornell–Larcker criterion results observed in Table 5 showed that the square root of the AVE was highest for each construct's correlation with itself. Furthermore, Group B's cross-loadings in Table 6 showed that each item loaded highest on its associated construct. Additionally, the HTMT resulted in all correlations being smaller than 1. Therefore, with the Fornell–Larcker criterion, cross-loading criterion and HTMT being met, the model for Group B was said to have discriminant validity. Furthermore, since the model had both convergent and discriminant validity, the model was valid for Group B. The evaluation of the measurement model concluded that the model used in this research study was valid and reliable for both groups A and B (Table 7).

Table 6 Results for cross loadings

Treatment group	A					B				
	BT	CT	ET	DPC	USD	BT	CT	ET	DPC	USD
BT1	0.95	0.44	0.49	−0.14	0.35	0.96	0.32	0.27	−0.06	0.09
BT2	0.97	0.46	0.37	−0.09	0.39	0.96	0.32	0.28	−0.11	0.13
BT3	0.96	0.45	0.43	−0.11	0.35	0.92	0.30	0.24	−0.12	0.07
CT1	0.31	0.75	0.57	−0.08	0.34	0.21	0.75	0.42	0.05	0.19
CT2	0.40	0.82	0.42	−0.23	0.29	0.25	0.77	0.47	−0.07	0.16
CT3	0.39	0.82	0.50	−0.16	0.31	0.28	0.79	0.44	−0.07	0.25
CT4	0.42	0.88	0.56	−0.10	0.31	0.29	0.84	0.57	−0.09	0.32
ET1	0.38	0.60	0.89	−0.04	0.38	0.25	0.53	0.88	−0.05	0.29
ET2	0.45	0.56	0.95	0.03	0.37	0.25	0.57	0.96	−0.12	0.33
ET3	0.40	0.57	0.91	−0.02	0.35	0.27	0.58	0.93	−0.06	0.36
DPC1	−0.12	−0.16	−0.03	0.90	−0.34	−0.08	0.03	−0.11	0.81	−0.36
DPC2	−0.02	−0.10	0.00	0.77	−0.19	0.02	−0.04	−0.09	0.86	−0.51
DPC3	−0.11	−0.17	0.01	0.83	−0.14	−0.13	−0.09	−0.10	0.85	−0.34
DPC4	−0.12	−0.14	−0.01	0.76	−0.20	−0.19	−0.12	−0.10	0.73	−0.31
USD1	0.38	0.40	0.36	−0.26	0.93	0.04	0.23	0.31	−0.48	0.94
USD2	0.28	0.36	0.38	−0.27	0.95	0.14	0.31	0.36	−0.47	0.95
USD3	0.40	0.33	0.37	−0.29	0.92	0.11	0.29	0.34	−0.38	0.91

Table 7 Results for heterotrait–monotrait ratio

Treatment group	A					B				
	BT	CT	ET	DPC	USD	BT	CT	ET	DPC	USD
BT										
CT	0.52					0.38				
ET	0.48	0.72				0.30	0.71			
DPC	0.13	0.23	0.04			0.14	0.13	0.14		
USD	0.40	0.44	0.44	0.30		0.11	0.34	0.39	0.52	

Table 8 Results on model fit

Treatment group	Constructs	*R* square
A	Cognitive trust	0.22
	Emotional trust	0.40
	User self-disclosure	0.24
B	Cognitive trust	0.11
	Emotional trust	0.37
	User self-disclosure	0.32

The structural model was used to assess relationship significance and model strength (Malhotra 2015). Three components were used to determine the structural integrity of the model: the model fit, the path coefficients and the effect sizes (Malhotra 2015). The first component was model fit, which required checking R square values loaded for each endogenous variable. An R square of 0.19 was considered a weak fit, 0.33 was considered a moderate fit, and 0.67 was considered a strong fit as seen in Table 8 (Malhotra 2015).

Group A's R square values were as follows: 0.22 for cognitive trust, a weak fit; 0.40 for emotional trust, a moderate fit; and 0.24 for user self-disclosure, a weak fit. Therefore, the model had an overall weak fit. Group B's R square values were as follows: 0.11 for cognitive trust, a weak fit: 0.37 for emotional trust, a moderate fit; and 0.32 for user self-disclosure, a weak fit. Therefore, the model had an overall weak fit.

The next component was path coefficients, which indicated the strength of the relationships between variables. Relationships were considered significant if the path coefficients were greater than 0.2 or less than −0.2 (Malhotra 2015).

Group A's path coefficients, presented in Table 9, were all greater than 0.2 or less than −0.2. Therefore, all relationships in the model for Group A were significant. The strongest relationship was between cognitive trust and emotional trust. The weakest relationship was shown to be between digital privacy concerns and user self-disclosure. Group B's path coefficients, observed in Table 9, were all greater than 0.2 or less than −0.2. Therefore, all relationships in the model for Group B were significant. The strongest relationship was

between cognitive trust and emotional trust. The weakest relationship was shown to be between emotional trust and user self-disclosure.

The last component of the structural model was the effect sizes, which were used to assess the effect of any changes made to the model (Malhotra 2015). The effect sizes were assessed using the output of the F square values found in Table 10. The effect size was considered weak when the value was between 0.02 and 0.15. It was considered moderate when the value was between 0.15 and 0.35 and was considered strong when the value was greater than 0.35 (Malhotra 2015).

Group A's F square values in Table 10 indicated that the majority of effect sizes were considered moderate. The exceptions were the effect sizes between cognitive trust and emotional trust, which were considered strong, and the effect size between digital privacy concerns and user self-disclosure, which were weak. Overall, given moderate effect sizes observed, it was concluded that the model was different to the original model with respect to the way it profiles the constructs.

Group B's F square values in Table 10 indicated that effect sizes range from weak to moderate to strong. The effect sizes between brand trust and cognitive trust, as well as emotional trust and user self-disclosure, was weak. The effect size between digital privacy concerns and user self-disclosure were moderate. On the other hand, the effect size between cognitive trust and emotional trust was considered strong. Overall, given the roughly moderate effect sizes, it was concluded that the model was different to the original model by Alashoor et al. (2017) with respect to the way it models the constructs.

Both models had a weak model fit, all relationships were significant and the model was similar to the original model. Thus, the model for both groups was structurally sound. Furthermore, path coefficients identifying significant relationships showed that the relationship between brand trust and cognitive trust and cognitive trust and emotional trust, as well as emotional trust and user self-disclosure, were more significant for Group A than Group B. In contrast, the relationship between digital privacy concerns and user self-disclosure was more significant for Group B. This revealed that trust was more significant for respondents exposed to a fictitious brand than those exposed to their preferred brand. Privacy concerns were greater for respondents exposed to their preferred brand than those exposed to a fictitious brand.

The following hypotheses were evaluated utilising the path coefficients in Table 11 for Groups A and B.

Table 9 Results for path coefficients

Treatment group	A					B				
	BT	CT	ET	DPC	USD	BT	CT	ET	DPC	USD
BT		0.47					0.33			
CT			0.63					0.61		
ET					0.40					0.31
DPC					−0.29					−0.44
USD										

Table 10 Results for f-square values

Treatment group	A					B				
	BT	CT	ET	DPC	USD	BT	CT	ET	DPC	USD
BT		0.28					0.12			
CT			0.66					0.59		
ET					0.21					0.14
DPC					0.11					0.29
USD										

Table 11 Results for significance of path coefficients

Treatment group	A		B	
	T-statistic	*P* values	*T*-statistic	*P* values
Brand trust—> cognitive trust	5.49	0.00	3.81	0.00
Cognitive trust—> emotional trust	12.78	0.00	12.26	0.00
Emotional trust—> user self-disclosure	4.67	0.00	3.85	0.00
Digital privacy concerns—> user self-disclosure	4.12	0.00	6.80	0.00

H_1: Brand trust positively influences Cape Town Internet banking users' cognitive trust when engaging with chatbots used in the South African banking industry

In Group A, the null hypothesis was rejected at the 5% level of significance, with a *p* value of 0.00 and a *t*-stat of 5.49. Therefore, it was concluded that brand trust had a positive influence on cognitive trust in Group A. In Group B, the null hypothesis was rejected at the 5% level of significance, with a *p* value of 0.00 and a *t*-stat of 3.81. Therefore, it was concluded that brand trust has a positive influence on cognitive trust in Group B.

H_2: Cognitive trust positively influences Cape Town Internet banking users' emotional trust when engaging with chatbots used in the South African banking industry

In Group A, the null hypothesis could be rejected at the 5% level of significance, with a *p* value of 0.00 and a *t*-stat of 12.78. Therefore, it was concluded that cognitive trust had a positive influence on emotional trust in Group A. In Group B, the null hypothesis was rejected at the 5% level of significance, with a *p* value of 0.00 and a *t*-stat of 12.26. Therefore, it was concluded that cognitive trust has a positive influence on emotional trust in Group B.

H_3: Emotional trust positively influences Cape Town Internet banking users' willingness to disclose personal information to chatbots used in the South African banking industry

In Group A, the null hypothesis could be rejected at the 5% level of significance, with a *p* value of 0.00 and a *t*-stat of 4.67. Therefore, it was concluded that emotional trust has a positive influence on user self-disclosure in Group A. In Group B, the null hypothesis was rejected at the 5% level of significance, with a *p* value of 0.00 and a *t*-stat of 3.84. Therefore, it was concluded that emotional trust has a positive influence on user self-disclosure in Group B.

H_4: Digital privacy concerns negatively influence Cape Town Internet banking users' willingness to disclose personal information to chatbots used in the South African banking industry.

The null hypothesis was rejected at the 5% level of significance, with a *p* value of 0.00 and a *t*-stat of 4.12. Therefore, it was concluded that digital privacy concerns have a negative influence on user self-disclosure. In Group B, the null hypothesis was rejected at the 5% level of significance, with a *p* value of 0.00 and a *t*-stat of 6.80. Therefore, it was concluded that digital privacy concerns have a negative influence on user self-disclosure in Group B.

The path coefficients in the structural model displayed the relationship between brand trust and cognitive trust, cognitive trust and emotional trust, as well as emotional trust and user self-disclosure having been more significant for Group A than Group B. While, the relationship between digital privacy concerns and user self-disclosure was more significant for Group B. This revealed that trust was more significant for respondents exposed to a fictitious brand than those exposed to their preferred brand. Privacy concerns were greater for respondents exposed to their preferred brand than those exposed to a fictitious brand.

An analysis of indirect effects revealed the significance of all indirect relationships. In this model, three indirect effects are observed in Table 12 and resulted in the following findings for Groups A and B.

The relationship between brand trust and emotional trust is significant at the 5% level of significance, with a *p* value of 0.00 and a *t*-stat of 4.84 for Group A and a *p* value of 0.00 and a *t*-stat of 3.31 for Group B. Therefore, it was concluded that brand trust has a positive influence on emotional trust. Additionally, the relationship between brand trust and user self-disclosure is significant at the 5% level of significance, with a *p* value of 0.00 and a *t*-stat of 3.20 for Group A and a *p* value of 0.00 and a *t*-stat of 2.13 for Group B. Therefore, it was concluded that brand trust has a positive influence on user self-disclosure. Furthermore, the relationship between cognitive trust and user self-disclosure is significant at the 5% level of significance, with a *p* value of 0.00 and a *t*-stat of 4.23 for Group A and a *p* value of 0.00 and a *t*-stat of 3.39 for Group B. Therefore, it was concluded that cognitive trust has a positive influence on user self-disclosure. These results indicated that, while all indirect effects were significant for Groups A and B, Group A's indirect effects were more significant than those of Group B.

To evaluate secondary research objectives, an analysis of variance (ANOVA) was conducted, which included a least squares difference (LSD) test to assess mean differences

Table 12 Results for significance of total indirect effects

Treatment group	A		B	
	T-statistic	*P* values	*T*-statistic	*P* values
Brand trust—> emotional trust	4.84	0.00	3.31	0.00
Brand trust—> user self-disclosure	3.20	0.00	2.13	0.03
Cognitive—> user self-disclosure	4.23	0.00	3.39	0.00

(Malhotra 2015). Furthermore, LSD results from Group A did not include the age range 51–60 due to an insignificant number of respondents. Thus, the LSD reporting for Group A consisted of 141 respondents rather than the total 142, as the age category of 51–60 was removed. Additionally, the *prefer not to answer* category from which no insights could be drawn was excluded in both Groups A and B. Three ANOVA tests were conducted comparing age and the constructs of digital privacy concerns, brand trust and user self-disclosure. Each ANOVA test was accompanied by an appropriate hypothesis to evaluate secondary objectives. The first ANOVA test compared age and digital privacy concerns with the following hypothesis and results in the findings observed in Tables 13 and 14.

H_{5a}: There is a difference in the level of digital privacy concerns between age categories among Cape Town Internet banking users

Significant differences was observed for both groups, between 18-35 and 35-50 (Group A) and 18-35 and 51-60 (Group B). In both cases the older age category experienced greater levels of privacy concerns

The second ANOVA test compared age and brand trust with the following hypothesis and rendered findings observed in Tables 15 and 16.

H_{5b}: There is a difference in the level of brand trust between age categories among Cape Town Internet banking users.

Group A's ANOVA test with an F-statistic of 3.78 and a p value of 0.01 provided sufficient evidence at the 5% level of significance that the means of the treatment Group A differed significantly with respect to brand trust. Furthermore, the LSD test showed that there was a significant difference between age groups 18–35 and 36–50 at the 5% level of significance, with a p value of 0.01 and a mean difference of 0.71. Furthermore, a significant difference is observed between age categories 18–35 and 60-older at the 5% level of significance, with a p value of 0.01 and a mean difference of 1.76. However, the difference between age categories 36–50 and 60-older proved insignificant. Therefore, age demographics between 18–35 and 36–50, as well as between 18–35 and 60-older, experienced different levels of brand trust that were statistically significant. Additionally, these

Table 13 Results of ANOVA conducted on the treatment groups A and B relating to digital privacy concerns

Treatment group	Construct		Sum of squares	Degrees of freedom	Mean square	*F*-statistic	Significance level
A	Digital privacy concerns	Between groups	20.21	4	5.05	6.98	0.00
		Within groups	99.23	137	0.72		
		Total	119.44	141			
B	Digital privacy concerns	Between groups	5.35	2	2.68	3.17	0.05
		Within groups	117.24	139	0.84		
		Total	122.59	141			

Table 14 Results of LSD test displaying mean difference between groups for treatment groups A and B

Treatment group	Construct	(I) Age	(J) Age	Mean difference (I–J)	Significance level
A	Digital Privacy Concerns	18–35	36–50	−0.59	0.00
			60-older	−0.05	0.87
		36–50	18–35	0.59	0.00
			60-older	0.54	0.11
		60-older	18–35	0.05	0.87
			36–50	−0.54	0.11
B	Digital Privacy Concerns	18–35	36–50	−0.34	0.15
			51–60	−1.01	0.03
		36–50	18–35	0.34	0.15
			51–60	−0.67	0.19
		51–60	18–35	1.01	0.03
			36–50	0.67	0.19

results indicated that the age category of 18–35 had a greater level of brand trust than that of respondents in the age categories of 35–50 and 60-older. Group B's ANOVA test with an F-statistic of 0.24 and a p value of 0.78 provided insufficient evidence at the 5% level of significance that the means of the treatment Group B differed significantly with respect to brand trust. Since no significant difference was observed, an LSD test was not conducted on Group B. Therefore, there was no statistical difference in the levels of brand trust with respect to age demographics observed in Group B. It was observed that only Group A displayed a significant difference between the age ranges. Group A observed a significance between age categories 18–35 and 35–50, as well as between 18–35 and 60-older. The results indicated that the younger age category experienced greater levels of brand trust (Table 15).

H_{5c}: There is a difference between age categories in the willingness of Cape Town Internet banking users to disclose personal information

It was observed that only Group A displayed a significant difference between the age categories. Group A showed a significant difference between age categories 18–35 and 35–50. These results indicated that the younger age category experienced greater levels of user self-disclosure. The next section presents conclusions on the findings.

Conclusions

The chatbot innovation presents an opportunity to extract personal information from consumers, which enables them to engage online in a customised fashion (Alashoor et al. 2017; Zumstein and Hundertmark 2017). However, this is greatly dependent on how much information consumers are willing to self-disclose, thus raising many digital privacy concerns (Papadopoulou et al. 2001). Nonetheless, this personalisation provides useful information for marketers, such that strategies can be tailored to a particular target audience. This type of personalisation also enhances the customer experience, leading to higher levels of satisfaction, loyalty and retention (Deloitte 2020). This research paper has explored the influence of digital privacy concerns and trust—to be brand, cognitive and emotional trust—on Cape Town Internet banking users' willingness to disclose personal information. This has been evaluated in the context of a highly competitive South African banking market (PwC 2017).

Objectives 1–4

Statistical analysis from PLS-SEM revealed that the relationship between brand trust and cognitive trust, cognitive trust and emotional trust, as well as the relationship between emotional trust and user self-disclosure, were more significant in the model for Group A. The relationship between digital privacy concerns and user self-disclosure proved more significant in the model for Group B. These results observed that digital privacy concerns were more significant and trust less significant in influencing user self-disclosure when respondents were exposed to their preferred banking brand as opposed to a fictitious banking brand. This could have been a result of banking brands experiencing low brand trust in South Africa (Collier 2012; Kessler et al. 2017). This indicates that the power of a brand alone will not considerably influence consumers to self-disclose. Rather, a bridge of trust is needed that encompasses brand, cognitive and emotional trust. Consumers need to feel that they can depend on the brand, rely on the technology itself and feel secure when engaging with chatbots to disclose personal information. This places importance on companies to ensure that their customer service builds trusting relationships that centre on a personalised experience that not only meets customers' needs but anticipates and exceeds them too. Furthermore, this presents an immense opportunity for small-medium enterprises (SMEs) to enter this space by ensuring consumers trust that their personal information is protected.

Objectives 5–7

Furthermore, findings were made through ANOVA testing. Digital privacy concerns were higher for the older age

Table 15 Results of ANOVA conducted on the treatment groups A and B relating to brand trust

Treatment group	Construct		Sum of squares	Degrees of freedom	Mean square	F-statistic	Significance level
A	Brand trust	Between groups	17.52	4	4.38	3.78	0.01
		Within groups	158.59	137	1.16		
		Total	176.11	141			
B	Brand trust	Between groups	0.55	2	0.28	0.24	0.78
		Within groups	156.38	139	1.13		
		Total	156.93	141			

category of 36–50 (Group A) and 51–60 (Group B) than the younger age category of 18–35 (Groups A and B). Thus, it was concluded that the older demographic experienced greater levels of digital privacy concerns. This could be a result of younger age groups using control measures when engaging with technology, such as making use of incognito tabs to protect their information search and an awareness of multi-factor authentication to safeguard disclosed information and saved credentials (Harding 2018 and Microsoft 2020). Additionally, the influence of age on brand trust displayed higher levels for the age category of 18–35 than for 36–50 and 60-older for Group A. This could be a result of consistent brand engagement on multiple platforms, with the younger population forming stronger bonds (Harding 2018). Overall, the age category of 18–35 displayed higher levels of user self-disclosure than that of 36–50 for Group A. This could be a result of the higher brand trust and lower digital privacy concerns experienced by the younger demographic.

Ultimately, chatbots offer an opportunity for brands, particularly in the banking sector, to gain more knowledge about their consumers, such that they can improve service quality. However, brands need to develop long-term, trust-based relationships to overcome the challenge of digital privacy concerns, such that users are more willing to self-disclose personal information.

Managerial implications

Companies using chatbots should focus on easing digital privacy concerns in order to improve engagement and lower privacy concerns. A major step towards this goal will be increasing cognitive trust by educating users on how chatbots operate and how their information will be protected. Furthermore, this study also concluded that the power of a brand is not enough for consumers to considerably influence self-disclosure. Rather, a bridge of trust, encompassing brand, cognitive and emotional, is needed. In this regard, digital-first new entrants into markets have an immense competitive advantage as traditional organisations struggle to pivot to the demands of the digital era (Deloitte 2020). The results showed that the younger demographic, particularly 18–35, showed lower levels of privacy concerns in both treatment groups, while displaying higher levels of brand trust and user self-disclosure in Group A. This may be attributed to the younger demographic's comfort level with technology (Landrum 2017) in contrast to the older demographic (Zeissig et al. 2017). Given that the older demographic may have fewer social media touch points with a brand and thus a lower brand trust, marketers should gear research to identifying how older users engage with their brand on digital platforms (Harding 2017). Overall, brands need an omni-channel presence to appeal to different segments in their target market and ensure that the channel chosen for a specific target has customised content.

Contribution to theory

In the study conducted by Awad and Krishnan (2006) and Baumer and Earp (2003), it was discovered that trust plays a pivotal role in the willingness of users to disclose personal information in online environments. However, both studies failed to explore trust as an independent construct. Moreover, despite the abundance of literature exploring the impact of trust on privacy concerns, trust was rarely explored in a multi-faceted fashion which this research study aimed to do by including cognitive, emotional and brand trust as separately tested constructs. Our study acknowledged that trust, particularly within the realms of technology and digital privacy concerns, comprises of elements such as; trust in reliability of the system to perform, a feeling of security when disclosing personal information and trust in a brand to ensure data security and efficiency in use (Alashoor et al. 2017; Hong-Youl 2004).

Furthermore, while the analytical model used was an adaptation of research by Alashoor et al. (2017), it is important to remember that in testing user willingness to disclose personal information, their study was conducted in a psychological framework. Our research has included brand trust to not only broaden the scope of managerial implications at an organisational level, but also to provide insights at a strategic marketing level. As previously mentioned, we acknowledge that brand trust forms an integral component to understanding user willingness to disclose personal information in online environments and including both a fictitious and branded bank in the questionnaire simulated this. The inclusion of brand trust as a dimension aligns with evidence that consumers differentiate by brand name and in undifferentiated markets, such as banking, competitiveness can be determined by customer experience and convenience (Hong-Youl 2004; Lam and Li 2017; PwC 2017; Al-Jabri 2015).

Lastly, chatbots have seen a large increase in investment due to the convenience they offer to consumers, the higher rates of retention observed when consumers use digital services and the costs saved in salaries and improved efficiencies. Therefore, the benefits accompanying chatbots make understanding the user behaviour surrounding the technology paramount for decision making in the context of an environment with increasing digital privacy concerns (Aguirre et al. 2015; Sahu et al. 2018; Zumstein and HundertmcKiark 2017). As consumers' digital worlds expand, so do their data points. This leaves brands with the choice of how to use and prompt customer data which can hold detrimental effects as seen in the Facebook Cambridge Analytica data breach (Frier 2018). We now know that the power of a brand is

not enough for consumers to considerably influence self-disclosure. Rather, a bridge of trust, encompassing brand, cognitive and emotional trust, is needed.

Limitations and future research

Future research could include a larger distribution of participants in order to include deeper insights on various demographic variables, like the level of technological education or income levels. The high level of inequality in South Africa that is correlated with education levels and technological education levels supports this (Van der Berg 2018), especially with the large growth potential in financial services adoption (Kessler et al. 2017). The sampling frame did not yield significantly diverse responses with respect to age. Respondents were mostly aged 18–35, which could be due to snowball sampling. As a result, the data are more reflective of individuals from a younger target market, whereas banks have target markets than span across all ages (PwC 2017). Moreover, age was the only demographic measured, which limited inferences made about the population. The study was limited to consumers who reside in Cape Town and therefore may not be generalisable to other regions, due to cultural and behavioural differences (Van Eeuwen 2017).

The three dimensions of trust tested in this study may not be the only determining factor in the willingness of users to disclose their personal information. Factors such as perceived risk, perceived benefits, data ownership, ethical use of data, privacy policy, involvement and transparency may also affect user willingness to disclose (de Cosmo et al. 2021; Følstad et al. 2021; Isaac and Hanna 2018; Nyugen and Khoa 2019). This model explores user trust but does not explore how to build that trust with the chatbot digital service through marketing efforts or communication, which will aid in overcoming trust barriers (Aguirre et al. 2015). Future research should look to address these opportunities. The model presented in this study may be modified in future research in order to explore the role of other factors that influence user willingness to disclose information to chatbots. Different kinds of private information can also be compared (e.g. banking information vs medical information) to categorise what information is more privacy-sensitive. Future research in the formulating of questions and the triggering of privacy concerns would be another welcome addition (Aguirre et al. 2015), as would further research on privacy-leakage (Xu et al. 2021). Additional research can focus on messaging specific themes (use of language, colloquialism and personalities) in order to create a more comfortable user experience that encourages the disclosing of information as well as the possibilities of chatbot to chatbot interactions (Hasal et al. 2021; de Cosmo et al. 2021). A comparison between chatbot interactions and live chat interactions (Rajaobelina 2021b) could also help to build an effectiveness measurement framework. Finally, emergent legislation like the General Data Protection Regulation (GDPR) in Europe or the Protection of Personal Information (POPIA) in South Africa where this study was based will shape the way people feel about disclosing personal information (potentially both positively and negatively) and hence future research will need to encompass a legislative viewpoint as this develops further globally (Coopamootoo et al. 2022; Netshakhuma 2020). This, however, also provides an opportunity to explore the impact that legislation in different countries has on trust and self-disclosure to chatbots.

References

Adam, M., M. Wessel, and A. Benlian. 2021. AI-based chatbots in customer service and their effects on user compliance. *Electronic Markets* 31 (2): 427–445.

Affrin, K.S., T. Mohan, and Y. Goh. 2018. Influence of consumers' perceived risk on consumers' online purchase intention. *Journal of Research in Interactive Marketing.* 12 (3): 309–327. https://doi.org/10.1108/JRIM-11-2017-0100.2020,December1.

Aguidissou, O.C., R. Shambare, and R. Rugimbana. 2017. Internet banking adoption in South Africa: The mediating role of consumer readiness. *Journal of Economics and Behavioral Studies.* 9 (5): 6–17.

Aguirre, E., A.L. Roggeveen, D. Grewal, and M. Wetzels. 2015. The personalization-privacy paradox: Implications for new media. *Journal of Consumer Marketing.* 33 (2): 98–110.

Alashoor, T., M. Boodraj, and K. Saffarizadeh. 2017. Conversational Assistants: Investigating Privacy Concerns, Trust, and Self-Disclosure. In *Proceedings from the Thirty Eighth International Conference on Information Systems*. 10–13 December 2017. Seoul, South Korea.

Al-Jabri, I.M. 2015. The intention to use mobile banking: Further evidence from Saudi Arabia. *South African Journal of Business Management.* 46 (1): 23–34.

Andersson, P., and L.G. Mattsson. 2015. Service innovations enabled by the "Internet of Things." *IMP Journal* 9 (1): 85–106.

AT Kearney. 2013. *Banking in a Digital World*. (Online) https://www.atkearney.com/documents/10192/3054333/Banking+in+a+Digital+World.pdf/91231b20-788e-41a1-a429-3f926834c2b0. 2018, March 16.

Awad, N.F., and M.S. Krishnan. 2006. The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly* 30 (1): 13–28.

Baumer, D., and J.B. Earp. 2003. Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM* 46 (4): 81–83.

Belen Saglam, R., J.R. Nurse, and D. Hodges. 2021. Privacy concerns in Chatbot interactions: When to trust and when to worry. In *International Conference on Human-Computer Interaction*, 391–399. Cham: Springer.

Benbasat, I., and S.Y. Komiak. 2004. Understanding customer trust in agent-mediated electronic commerce, web-mediated electronic

commerce, and traditional commerce. *Information Technology and Management* 5 (1–2): 181–207.

Benbasat, I., and S.Y. Komiak. 2006. The effects of personalization and familiarity on trust and adoption of recommendation agents. *MIS Quarterly* 30 (4): 941–960.

Brandtzæg, P. B., and A. Følstad, 2017. Why people use chatbots. *Proceedings of the 4th International Conference on Internet Science.* 22–24 November, 2017. Thessaloniki, Greece.

Brown, M., and R. Muchira. 2004. Investigating the relationship between Internet privacy concerns and online purchase behavior. *Journal of Electronic Commerce Research* 5 (1): 62–70.

Bruner, G.C. 2013. *Marketing scales handbook*, 7th ed. Fort Worth, Texas: GCBII Productions.

Burden, D., M. Savin-Baden, G. Tombs, and C. Wood. 2013. It's almost like talking to a person': Student disclosure to pedagogical agents in sensitive settings. *International Journal of Mobile and Blended Learning* 5 (2): 78–93. https://doi.org/10.4018/jmbl.2013040105.

Businesstech. 2020. *Standard Bank, Absa and FNB respond to massive data breach in South Africa.* https://businesstech.co.za/news/banking/427232/standard-bank-absa-and-fnb-respond-to-massive-data-breach-in-south-africa/. 2020, November 28.

Business Report. 2018. *Absa introduces WhatsApp Banking - A first for SA*. [Online] Available: https://www.iol.co.za/business-report/companies/absa-introduces-whatsapp-banking-a-first-for-sa-15952911. 2018, August 30.

Cai, L. and C. Hsu. 2009. Brand knowledge, trust and loyalty—A conceptual model of destination branding. In *Proceedings of the International CHRIE Conference on "Bridging the Visions of Hospitality and Tourism Education Worldwide"*. 29 July–1 August 2009 (pp. 1–10). (Online). http://scholarworks.umass.edu/refereed/Sessions/Friday/12. 2018, March 10.

Chattaraman, V., W. Kwon, J.E. Gilbert, and K. Ross. 2019. Should AI-Based, conversational digital assistants employ social- or task-oriented interaction style? A task-competency and reciprocity perspective for older adults. *Computers in Human Behavior.* 90: 315–330.

Chellappa, R.K., and R.G. Sin. 2005. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management* 6 (2): 181–202.

Coelho, P.S., P. Rita, and Z.R. Santos. 2018. On the relationship between consumer-brand identification, brand community and brand loyalty. *Journal of Retailing and Consumer Services.* 1: 1. https://doi.org/10.1016/j.jretconser.2018.03.011.

Coetzee, J., H. Van Zyl, and M. Tait. 2013. Perceptions of service quality by clients and contact personnel in the South African retail banking sector. *Southern African Business Review* 17 (1): 1–22.

Collier, M. 2012. *5 Reasons Why You Need to Stop Marketing and Start Teaching*. (Online) http://www.mackcollier.com/building-trust-through-teaching/. 2018, August 30.

Coopamootoo, K.P., M. Mehrnezhad and E. Toreini. 2022. "I feel invaded, annoyed, anxious and I may protect myself": Individuals' Feelings about Online Tracking and their Protective Behaviour across Gender and Country. arXiv:2202.04682.

Corritore, C.L., B. Kracher, and S. Wiedenbeck. 2003. On-line trust: Concepts, evolving themes, a model. *International Journal of Human-Computer Studies* 58: 737–758. https://doi.org/10.1016/S1071-5819(03)00041-7.

de Cosmo, L.M., L. Piper, and A. Di Vittorio. 2021. The role of attitude toward chatbots and privacy concern on the relationship between attitude toward mobile advertising and behavioral intent to use chatbots. *Italian Journal of Marketing* 2021 (1): 83–102.

Deloitte. 2020. *Connecting with meaning. Hyper-personalizing the customer experience using data, analytics, and AI.* https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/deloitte-analytics/ca-en-omnia-ai-marketing-pov-fin-jun24-aoda.pdf. 2020, November 30.

Degirmenci, K. 2020. Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management* 50: 261–272.

Dinev, T., and P. Hart. 2006. An extended privacy calculus model for E-commerce transactions. *Information Systems Research* 17 (1): 1.

Featherman, M.S., and N. Hajli. 2015. Self-service technologies and e-service risks in social commerce era. *Journal of Business Ethics* 139 (2): 251–269.

Flew, T. 2018. Platforms on Trial. *InterMedia* 46 (2): 24–29.

Følstad, A., T. Araujo, E.L.C. Law, P.B. Brandtzaeg, S. Papadopoulos, L. Reis, M. Baez, G. Laban, P. McAllister, C. Ischen, and R. Wald. 2021. Future directions for chatbot research: An interdisciplinary research agenda. *Computing* 103 (12): 2915–2942.

Følstad, A., C.B. Nordheim, and C.A. Bjørkli. 2018. What makes users trust a chatbot for customer service? An exploratory interview study. In *International conference on internet science*, 194–208. Cham: Springer.

Frier, S. 2018. Facebook just doubled the number of people exposed in data Breach. *Time.* 4 April. (Online). http://time.com/money/5228277/facebook-cambridge-analytica-data-breach-numbers/. 2018, April 29.

Galletta, D.F., P.B. Lowry, and G.D. Moody. 2014. When trust and distrust collide online: The engenderment and role of consumer ambivalence in online consumer behavior. *Electronic Commerce Research and Applications* 13 (4): 266–282. https://doi.org/10.1016/j.elerap.2014.05.001.

George, A., and G.S.G. Kumar. 2014. Impact of service quality dimensions in internet banking on customer satisfaction. *Decision* 41 (1): 73–85.

Global Commission on Internet Governance (GCIG). 2015. *Toward a Social Compact for Digital Privacy and Security*. Waterloo, Canada: Centre for International Governance Innovation and The Royal Institute for International Affairs (Online). https://ourinternet-files.s3.amazonaws.com/publications/GCIG_Social_Compact.pdf. 2018, April 29.

Gözükara, I., and N. Çolakoğlu. 2016. A research of generation Y Students: Brand Innovation, Brand Trust and Brand Loyalty. *International Journal of Business Management and Economic Research.* 7 (2): 603–611.

Gong, X., K.Z.K. Zhang, S.J. Zhao, and M.K.O. Lee. 2016. The Effects of cognitive and emotional trust on mobile payment adoption: A trust transfer perspective. *AISeL Proceedings.* 350: 1.

Gnewuch, U., S. Morana and A. Madche. 2017. Towards designing cooperative and social conversational agents for customer service. *Proceedings from the International Conference on Information Systems.* 6 December - 13 December 2017 [Online]. http://aisel.aisnet.org/icis2017/HCI/Presentations/1/. 2018, April 30.

Han, M.C. 2021. The impact of anthropomorphism on consumers' purchase decision in Chatbot commerce. *Journal of Internet Commerce.* 20 (1): 46–65.

Harding, S. 2017. *Trends 2018*. (Report 0018A). London, United Kingdom: Mindshare Futures.

Hasal, M., J. Nowaková, K. Ahmed Saghair, H. Abdulla, V. Snášel, and L. Ogiela. 2021. Chatbots: Security, privacy, data protection, and social aspects. *Concurrency and Computation: Practice and Experience* 33 (19): 6426.

Hong-Youl, H. 2004. Factors influencing consumer perceptions of brand trust online. *Journal of Product & Brand Management.* 13 (5): 329–342. https://doi.org/10.1108/10610420410554412.

Hughes, A.M. 1994. *Strategic Database Marketing: The Masterplan for Starting and Managing a Profitable, Customer- Based Marketing Program*. Chicago: Probus Publishing.

Isaac, J., and M.J. Hanna. 2018. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer* 51 (8): 56–59.

Jang, M., Y. Jung, and S. Kim. 2021. Investigating managers' understanding of chatbots in the Korean financial industry. *Computers in Human Behavior* 120: 106747.

Javidina, M., M. Maadi, and M. Maadi. 2016. Identification of factors influencing building initial trust in e-commerce. *Iranian Journal of Management Studies* 9 (3): 483–503.

Jian, J.Y., A.M. Bisantz, and C.G. Drury. 2000. Foundations for an empirically determined scale of trust in automated systems. *International Journal of Cognitive Ergonomics* 4 (1): 53–71.

Jünger, M. and M. Mietzner. 2020. Banking goes digital: The adoption of FinTech services by German households. *Finance Research Letters* 34: 1.

Kaczorowska-Spychalska, D. 2019. How Chatbots Influence Marketing. *Sciendo Management.* 23 (1): 251–270.

Kanter, J. 2018. Trust in Facebook has spectacularly nosedived after its enormous data breach. *Business Insider* (Online). http://www.businessinsider.com/facebook-trust-collapses-after-cambridge-analytica-data-scandal-2018-4?IR=T. 2018, April 29.

Kessler, K., Ikdal, A.S., Naidoo, E., Portafix, A., Hendrickson, J., Boje, A. & Rabec, D. 2017. Improving Financial Inclusion in South Africa. *Boston Consulting Group* (Online). https://www.bcg.com/publications/2017/globalization-improving-financial-inclusion-south-africa.aspx. 2018, August 30.

Khan, A., S. Ranka, C. Khakare, and S. Karve. 2019. NEEV: An education informational chatbot. *International Research Journal of Engineering and Technology* 6 (4): 492–495.

Kharpal, A. 2017. Amazon's Alexa Stole the Show at CES in a Bid to Become the Internet of Things Operating System. *CNBC*. 6 January (Online). https://www.cnbc.com/2017/01/06/ces-2017-amazon-alexa-stole-the-show-a-bid-to-become-the-iot-operating-system.html. 2018, September 03.

Lam, H.C. & Li, Q. 2017. Does electronic customer relationship management affect customer satisfaction and trust. Masters in Marketing. Thesis. University of Gavle.

Landrum, S. 2017. *Millennials, Trust And Internet Security* (Online). https://www.forbes.com/sites/sarahlandrum/2017/06/28/millennials-trust-and-internet-security/#1bfb8735555e. 2018, August 30.

Malhotra, N.K., S.S. Kim, and J. Agarwal. 2004. Internet user's information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* 15 (4): 336–355.

Malhotra, N.K. 2015. *Essentials of Marketing Research: A Hands-On Orientation*, 1st ed. New York: Pearson.

Martins, A. 2017. Cognitive and affective brand trust: an approach to baby care category. Masters dissertation, Porto School of Economics and Management (FEP). Accessed 2 Feb 2022.

Mazurek, G., and K. Małagocka. 2019. Perception of privacy and data protection in the context of the development of artificial intelligence. *Journal of Management Analytics* 6 (4): 344–364.

McDonald, W. 2014. *Your Path to a World-Class Customer Experience* (Online). https://www.ttec.com/articles/bankings-most-important-currency-customer-trust. 2020, November 15.

Mietzner, M., and M. Jünger. 2020. Banking goes digital: The adoption of FinTech services by German households. *Finance Research Letters* 34: 1.

Mendoza, N.F., 2020. Data privacy: What consumers want businesses to know (Online). https://www.techrepublic.com/article/data-privacy-what-consumers-want-businesses-to-know/. 2020, November 30.

Moneta, J. and L. Sinclair. 2020. *COVID-19 has accelerated digital adoption—The time to transform is now* (Online). https://www.thinkwithgoogle.com/intl/en-ssa/future-of-marketing/digital-transformation/covid-accelerated-digital-adoption/. 2020, November 30.

Moyo, A. 2017. *ABSA Banks on Robotics, Artificial Intelligence*. 2 May (Online). https://www.itweb.co.za/content/JOlx4zMkyKDv56km. 2018, March 15.

Mukherjee, A., and P. Nath. 2003. A model of trust in online relationship banking. *International Journal of Bank Marketing* 21 (1): 5–15. https://doi.org/10.1108/02652320310457767.

Müller, A. 2016. *Be careful what you tell a chatbot - it could come back to bite you* (Online). https://venturebeat.com/2016/04/23/be-careful-what-you-tell-a-chatbot-it-could-come-back-to-bite-you/. 2018, March 10.

Netshakhuma, N.S. 2020. Assessment of a South Africa national consultative workshop on the Protection of Personal Information Act (POPIA). *Global Knowledge, Memory and Communication* 69 (1/2): 58–74.

Ng, M., K.P. Coopamootoo, E. Toreini, M. Aitken, K. Elliot and van A. Moorsel. 2020. Simulating the effects of social presence on trust, privacy concerns & usage intentions in automated bots for finance. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* IEEE: 190–199

Norberg, P.A., D.R. Horne, and D.A. Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behavuors. *Journal of Consumer Affairs* 41 (1): 100–126.

Nowak, G., and J. Phelps. 1995. Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Interactive Marketing* 9 (3): 46–60.

Nyugen, H.M., and B.T. Khoa. 2019. The relationship between the perceived mental benefits, online trust, and personal information disclosure in online shopping. *Journal of Asian Finance, Economics and Business.* 6 (4): 261–270.

Papadopoulou, P., A. Andreou, P. Kanellis, and D. Martakos. 2001. Trust and relationship building in electronic commerce. *Internet Research* 4 (11): 322–332. https://doi.org/10.1108/10662240110402777.

Pantano, E., and G. Pizzi. 2020. Forecasting artificial intelligence on online customer assistance: Evidence from chatbot patents analysis. *Journal of Retailing and Consumer Services* 55: 102096.

Phelps, J., Nowak, G., & Ferrell, E. 2000. Privacy concerns and consumer willingness to provide personal information. *Journal of public policy & marketing*, 19 (1), 27–41

Pont, M., and L. McQuilken. 2002 Testing the Fit of the BANKSERV Model to BANKPERF Data. *Proceedings from the Australian and New Zealand Marketing Academy Conference*. 2–4 December. Dunedin, New Zealand. 861–867.

PricewaterhouseCooper (PwC). 2017. *South Africa- Major Banks Analysis* (Online). https://www.pwc.co.za/en/assets/pdf/major-banks-analysis-sept-2017.pdf. 2018, March 13.

Przegalinska, A., L. Ciechanowski, A. Stroz, P. Gloor, and G. Mazurek. 2019. In bot we trust: A new methodology of chatbot performance measures. *Business Horizons* 62 (6): 785–797.

Radziwill, N.M. and M.C. Benton. 2017. *Evaluating Quality of Chatbots and Intelligent Conversational Agents*. ArXiv preprint arXiv:1704.04579.

Rajaobelina, L., Brun, I., Kilani, N. & Ricard, L. 2021a. Examining emotions linked to live chat services: The role of e-service quality and impact on word of mouth. *Journal of Financial Services Marketing*.Vancouver: 1–18.

Rajaobelina, L., S. Prom Tep, M. Arcand, and L. Ricard. 2021b. Creepiness: Its antecedents and impact on loyalty when interacting with a chatbot. *Psychology & Marketing* 38 (12): 2339–2356.

Rajapaksha, D.S., A.K. Warapura, H.P Ranawaka, P.S.S.J. Fernando, K.T.S. Kasthuriarachchi, and D. Wijendra. 2014. *Proceedings from Sri Lanka Institute of Information Technology.* December 2014. (Online). https://www.researchgate.net/profile/Sanvitha_

Kasthuriarachchi/publication/272623530_Automated_Customer_Care_Service_System_for_Finance_Companies/links/54eab4750cf25ba91c83bb20.pdf. 2018, March 13.

Rajgopaul, D, 2020. *Standard Bank launches WhatsApp chatbot to keep customers informed* (Online). https://www.iol.co.za/business-report/companies/standard-bank-launches-whatsapp-chatbot-to-keep-customers-informed-46781059 [2020, 29 November].

Redlinghuis, A., and C. Rensleigh. 2010. Customer perceptions on internet banking information protection. *SA Journal of Information Management* 12 (1): 1–6.

Ritter, D.S. 1993. *Relationship Banking: Cross- selling the Bank's Products & Services to Meet Your Customer's Every Financial Need*. Chicago, Illinois: Bankers Pub. Co.

Rodríguez Cardona, D., A. Janssen, N. Guhr, M.H. Breitner, and J. Milde. 2021. A Matter of Trust? Examination of Chatbot Usage in Insurance Business. In *Proceedings of the 54th Hawaii International Conference on System Sciences*: 556.

Sahu, N., H. Deng, and A. Mollah. 2018. Investigating the critical success factors of digital transformation for improving customer experience. In *International Conference on Information Resources Management (CONF-IRM)*. Association For Information Systems.

Sebastian, I. M., Ross, J. W., Beath, C., Mocker, M., Moloney, K. G., & Fonstad, N. O. 2017. How big old companies navigate digital transformation. *MIS Quarterly Executive*, 16 (3), 197–213.

Scherer, A., N.V. Wunderlich, and F. Wagenheim. 2015. The value of self-service: Long-term effects of technology-based self-service usage on customer retention. *MIS Quarterly.* 39 (1): 177–200.

Shapshak, T. 2015. *Why WhatsApp Is South Africa's Favourite App* (Online). https://www.forbes.com/sites/tobyshapshak/2015/09/04/why-whatsapp-is-south-africas-favourite-app/#49201ce52e2b. 2018, August 30.

Sheehan, B., H.S. Jin, and U. Gottlieb. 2020. Customer service chatbots: Anthropomorphism and adoption. *Journal of Business Research* 115: 14–24.

Song, M., X. Xing, Y. Duan, J. Cohen, and J. Mou. 2022. Will artificial intelligence replace human customer service? The impact of communication quality and privacy risks on adoption intention. *Journal of Retailing and Consumer Services* 66: 102900.

Tan, M., and T.S.H. Teo. 2000. Factors Influencing the Adoption of Internet Banking. *Journal of the AIS.* 1 (11): 1.

Upward, J. 2014. *How technology can help small businesses become big brands* [Online]. https://www.theguardian.com/media-network/media-network-blog/2014/aug/14/tech-data-small-businesses-micro-enterprises-new-markets. 2018, August 30.

Vance, A., C. Elie-dit-cosaque, and D.W. Straub. 2008. Examining trust in information technology artifacts: The effects of system quality and culture. *Journal of Management Information Systems* 24 (4): 73–100.

Van den Broeck, E., and K. Poels. 2019. Chatbot advertising effectiveness: When does the message get through? *Computers in Human Behavior.* 98: 150–157.

Van der Berg, S. 2018. *The Two-Way Street between Poverty and Education* (Online). https://projectrise.news24.com/two-way-street-poverty-education/. 2018, August 30.

Van Eeuuwn, M. 2017. *Mobile conversational commerce: Messenger chatbots as the next interface between businesses and consumers*. Dissertation. University of Tweente (Online). http://essay.utwente.nl/71706/1/van%20Eeuwen_MA_BMS.pdf. 2018, March 10.

Venter, P., and M. Jansen van Rensburg. 2014. *Strategic Marketing: Theory and application for competitive advantage*, 2nd ed., 20–21. Cape Town: Oxford University Press.

Wang, C., H. Wang, and M.K.O. Lee. 1998. Consumer privacy concerns about internet marketing. *Communications of the ACM.* 41 (3): 1.

Watson, H.J., and C. Nations. 2019. Addressing the growing need for algorithmic transparency. *Communications of the Association for Information Systems* 45 (1): 26.

Widener, A., and S. Lim. 2020. Need to belong, privacy concerns and self-disclosure in AI chatbot interaction. *Journal of Digital Contents Society* 21 (12): 2203–2210.

Williams, M., J.R. Nurse, and S. Creese. 2019. Smartwatch games: Encouraging privacy-protective behaviour in a longitudinal study. *Computers in Human Behavior* 99: 38–54.

Xu, Q., C. Xu, and L. Qu. 2021. Privacy monitoring service for conversations. In *Proceedings of the 14th ACM International Conference on Web Search and Data Mining:* 1093–1096.

Zeissig, E., C. Lidynia, L. Vervier, A. Gadeib, and M. Ziefle. Online Privacy Perceptions of Older Adults. In *Proceedings from Third International Conference Human Aspects of IT for the Aged Population*. 9–14 July 2017. Vancouver, Canada.181–200.

Zeng, F., et al. 2021. Does self-disclosure matter? A dynamic two-stage perspective for the personalization-privacy paradox. *Journal of Business Research.* 124: 667–675.

Zumstein, D., and S. Hundertmark. 2017. Chatbots- An Interactive Technology for Perosnaliased Communication, Transactions and Services. *International Journal WWW/Internet* 15 (1): 96–109.