Université de Neuchâtel
Faculté des sciences économiques

Research on Intention versus Actual disclosure through dual process of privacy decision-making on Artificial Intelligence Assistants

Master thesis submitted to the Faculty of Economic sciences
Institute Economic Research
University of Neuchâtel

For the Master in Innovation science
by

Jessica RAVOMANANA LAN YON SUE

Supervised by:
Prof Valentin Bezençon, University of Neuchâtel
Ertuğrul Uysal, Teaching and Research Assistant, University of Neuchâtel

Neuchâtel, July 2022

Faculté des sciences économiques
Avenue du 1er-Mars 26
CH-2000 Neuchâtel
www.unine.ch/seco

LETTRES ET SCIENCES HUMAINES
SCIENCES
DROIT
SCIENCES ECONOMIQUES

ABSTRACT

The intention-actual disclosure gap has been explored in previous studies and scenarios. More importantly, the Elaboration Likehood Model introduces a dual route which initiates the disclosure of decision-making. Researchers argue that people's changing attitudes by sharing personal information are the result of rational thinking and other biased or heuristic cues. These elements implied the existing discrepancies between people's expressed intentions and their actual behavior. However, those theories have not been reviewed on the Artificial Intelligence Assistance (AIA) aspect yet. Thus, we conducted an empirical survey with 109 respondents. By using a regression analysis, we tested the impact of privacy concern and perceived benefit calculation (rational route) and the social-informational cues (heuristic route) on participant's willingness to surrender their personal information. Then, we investigate how salient is the influence of their hypothetical choice on actual disclosure decision. Our findings show that the rational calculus is predominant on the disclosure intentions compared to actual disclosure behaviors. In comparison, less rational process (i.e., relationship length and information to privacy protection) influence directly and indirectly the actual behavioral disclosure. We also identify that actual disclosure is embedded by intention. This study develops the antecedents of the two specific paths according to an AIA context and investigates beyond the privacy paradox theory.

Keywords: Artificial intelligence assistant, Elaboration Likehood model, privacy paradox, rational calculus, privacy concern, perceived benefit, information to privacy protection, relationship length.

TABLE OF CONTENTS

1. **INTRODUCTION**

The use of Artificial Intelligence Assistants (AIA) became the start of many changes in people's daily lives, mostly through the ease of the working process and information's access.
Basically, artificial intelligence assistants are known as speech-enabled technologies that provide assistance to perform different tasks (Hauswald et al., 2015) such as information research, entertainment, or scheduling. They offer a whole package of different services, size features, contextual use like at work, or only at home and applied to different devices (smartphones, tablets, cars…).
To some extent, AI systems gather tremendous data from their users to ensure quality and efficiency of their performance. The latter have been the core tool of many industries and labeled as customization (Ansari and Mela, 2003; Winer, 2001). For companies, offering personalized products or services depends mostly on the customer's personal information and preferences (Riemer, K and Toz, C. 2010; Chellappa, R.K and Sin, R. 2005).

Whereas, collecting personal information implies that users can be at risk of losing their privacy. This cutting-edge technology enables issues such as persistent surveillance, misused data or discrimination among users (Bartneck, C. et al., 2021). Therefore, people develop concern over their privacy towards such devices (Arora, N et al, 2008). Previous work posits how consumers are favorable around the digital assistant's home security attributes but still adamant over their privacy (Shields, 2018). Such worries may trigger people to withhold their personal data. This predicament implies reviewing different factors that influence self-disclosure.
Different researchers argue that an individual's decision is supported by rational, semi-rational thinking or even non-rational ways. Furthermore, a specific study on the privacy paradox (Barth, S et al., 2017) presents two disparities of decision-making assessments over self-disclosure. One on one hand, the first assessment involves a rational calculus between risk-benefit also known as the privacy calculus, while these attributes influence negatively and positively the individual's intention and actual disclosure behavior (Culnan and Armstrong, 1999). One the other hand, biased and heuristic cues may appear to influence this designated trade-off in the process. The second assessment nullifies the risk-benefit calculation, whereby estimating privacy threat is not even prominent.

If rational factors are observed to be at the center of this model to determine self-disclosure, heuristic cues are located at the peripheral view. We propose one model, the Elaboration Likelihood model (Petty, R.E and Cacippo, 1980) that works on all these processes and divides them in two paths. Different studies and context, such as in advertising and marketing (Bitner, Mary J., and Carl, 1985), in healthcare (Angst and Agarwal, 2009), in social media (Pee, L.G 2012; Wang, L. et al., 2019), applied these underlying mechanisms on intentions disclosure. Researchers argue that intention is the most significant predictor of actual behavioral disclosure which result in its use in many privacy studies to examine information disclosure (Ajzen, 1988, 1991; Fishbein, 1980; Fishbein and Ajzen, 1975; Rogers, 1983; Triandis, 1980). Nonetheless, empirical research admits an actual gap between people's actual behavior and their expressed intention to share information (Norberg et al., 2007).

Our work explores the dual processes in privacy decision-making leading towards disclosure choices preferences (RQ1). Furthermore, we investigate the intention-behavior gap by determining the power of intention to predict actual disclosure (RQ2). This gap has already been investigated through different theoretical works and aspects, aside from the AIA scenario, which has broadened past studies.

Furthermore, the dichotomy between intention and actual disclosure is not fully explained by the privacy paradox. Our study aims to extend this theory by integrating ELM to offer a clear explanation for the gap between users' intentions and their behavior. We argue that intention is affected by rational calculus while actual disclosure is influenced not only by intention but also by heuristic cues. Determining the antecedents is potentially the best method to understand AIA users' privacy decision-making practices.

To have a clear understanding of the literature review, we will discuss the ELM and privacy paradox theory in detail. We will propose 5 hypothetical statements based in past works and later on, our methodology will present a regression analysis to test those hypotheses. Finally, the findings will be arranged to copy the mechanism of privacy decision-making, potential limitation, and development for future research.

2. LITERATURE REVIEW

2.1. Privacy Calculus Theory

Earlier traditional economic literature on privacy and disclosure supported rational perspectives in self disclosure. Thus, they maintain that decisions are the result of conscious operation, weighing up utility gains versus losses in sharing information. This objective process reminds the idea of the privacy calculus theory (Culnan and Bies, 2003). The theory explains perceived benefits and costs are two main predictors for disclosure. Therefore, an individual's intent and behavior to surrender personal information are driven by perceived benefits which outweigh perceived risks (Li, Hong & Zhu, 2016).

2.2. Elaboration Likelihood Model (ELM)

The dual process

Other studies reveal that individuals' risk-benefit calculation over disclosure behavior is not utterly a thoughtful process, somewhat Kaufman (Kaufman, 1999) indicates that decisions-making are subject to heuristic cues. To completely explain the fundamental principles on disclosure decisions in an Artificial Intelligence (AI) system-based context, we present the Elaboration Likelihood Model (ELM) (Chaiken, 1980) that aims to reunite both perspectives (i.e. rational and heuristic).

This model implies that people assess information through a dual process: the central route and the peripheral route. The central route relies on analytic and cognitive approach upon judging relevant information (Chen, S., Duckworth, K., & Chaiken, S. (1999). In the privacy aspect, the central route is mainly in accordance with the risk-benefit of the privacy calculus as mentioned previously.

Under the peripheral route, decisions are subject to heuristics. Heuristics are mental process where individuals might use inferences towards their surroundings, apply their intuition and insights (Alexanderson, G. L., & Polya, G., 1979), or refer to their experiences (Bell, E. T., & Polya, G., 1945; van Stralen, D., & Mercer, T., 2021).

The heuristic cues

Informational cue

As the quantity of information to deal with might be tremendous, people's mental capacities are limited to process all of them and heuristics cues are relevant to save resources. In addition, the nature of these cues might be verbal (Peacock & Ekstrom., 2018) and non-verbal (Mukherjee., 2012). Thus, people might use primary information as an anchor to make decision. This process is labelled as the anchoring heuristic (Tversky & Kahneman, 1974). (Stewart et al., 2004) explain that it is the likelihood of people to base their judgement on an initial information or their own knowledge (Tullis., 2018) and neglect subsequent information. Moreover, memory is associated to the anchor (Coon & Mitterer., 2008). Thus, anchoring heuristic is triggered by external cue or stimulus which is associated to an internal state or focus awareness (Bucy, 2017).

Accordingly, the innovative devices (i.e, AIA) offer diverse cues and technological characteristics which enable to further guide judgments and evaluations of service quality (Niether & Wiegand., 2017; Metzger, & Flanagin AJ., 2015; Metzger & Flanagin., 2013) such as privacy policy. Therefore, companies establish data protection and informed their consumers for transparency (DiPiazza & Eccles., 2002) and ethical purpose (Turilli & Floridi., 2009). In sum, companies' responsability activity (i.e., privacy protection) have an important effect on consumers' attitudes and their behavioral choice for further interaction (Aktar 2011, Campbell and Kirmani 2000). In accordance with the anchoring heuristic, researchers maintain that people save effort and operate an active judgement based on those "pre-existing information" without a thorough evaluation (Metzger and al., 2010). In a context where the information flood, people might count on such external and primary informational cues as anchor to convey the credibility of their decision.

Similarly, privacy studies shows that information may decrease thoughtful decision-making process, as more knowledge actually reduces concern (Dommeyer and Gross, 2003, Uslaner, 2004). More importantly, researchers argue that privacy knowledge serves as a reinforcing mechanism for those who are most (or least) concerned about their privacy to protect them (Park et al., 2012). For instance, those who are less or more worried about their privacy conceive privacy protection knowledge as an anchor to give their judgements. As higher level of knowledge about the collection and use of personal data will fill their lack of concern or strengthen their protective behavior (Park et al., 2012). Therefore, we will investigate information about privacy protection as an informational cue in the peripheral view.

Social cue

Additionally, another particular aspect for less rational process implies the social heuristic (Hertwig, & Herzog., 2009), whereby making decision involved for instance the relationship with other actors and knowledge is gained through the observation of such actor. Likewise, the "learning by doing" concept is a reference for future decision. Researchers argue that individuals tend to reenact familiar decision through the experience of previous situations (Schirrmeister and al., 2020). Moreover, this learning process takes a longer time of discovery (John Dewey, 2021). Social psychology study indicates that individuals with long lasting relationships are more likely to collect information about the other parties (Berscheid et al. 1976). Moreover, researchers also maintain that people have better opportunities to predict behavior, as past situations might be basic foundations for following ones within a long time (Nicholson et al., 2001).

Thus, past works propose duration as a cue for triggering the social heuristic by inferring decision (Yeung & Soman., 2006). These researchers propose that individual count on duration heuristic cue to facilitate the evaluation process. To assess how easily duration can be used as a cue, we distinguish the evaluability of an attribute (Hsee, 1996; Hsee et al. 1999). Previous studies mention that an attribute is difficult to process if the individual lacks knowledge about that attribute's practical range, objective reference point, and value distribution (Yeung, C., & Soman, D., 2007). Overall, duration gets all these features. For instance, the time period warranty of Amazon's smart personal devices varies from 90 days to 1 year (Amazon, 2022). Furthermore, this time period depends on the product range, while consumers obtain extended services following the longer duration. In addition, this duration leads the consumer on a relational process with the product/services providers, which later form a relationship value (Yeung, C., & Soman, D., 2007).

Thus, these advantages, either hedonistic or utilitarian (Chitturi et al., 2008), reflect the valuable aspect of the time and its dependency impact on the relational concept (Swan & Gill., 1997). Therefore, we assess that the duration spends with either the service providers or the product is an important cue that activates social heuristic along the relationship journey with the consumers. Hence, this work will investigate the relationship length build with the AIA as a cue.

Subsequently, while making decisions, the dual process can operate either at the same time or separately. However, the ELM model has been used in different studies to only predict the hypothetical result (i.e., intention) after high thought (i.e., central route) or low thought (i.e., peripheral route) on the message. Hence, the model lacks to determine the actual disclosure decision with those antecedents in the privacy field.

2.3. Privacy paradox

Crossing the recent and former definitions from the literature, self-disclosure engages to reveal one self's personal information, whereby exposing one thoughts, attitudes, or emotions to other parties (Catona and Greene, 2015; Pearce and Sharp, 1973).

Studies about individuals' actual disclosure behaviors have been far more limited than those on behavioral intentions (Idris, 2018). Several researches have described intentions as the ultimate factor for different range of behaviors such as weight loss (e.g., Bagozzi & Warshaw, 1990), academic achievement (e.g., Sheeran, Orbell, & Trafimow, 1999) or smoking (e.g., Norman, Conner, & Bell, 1999).

Behavioral intentions are subject to a probability that the individual will perform the behavior (Fishbein and Ajzen, 1975). However, this probability does not provide full accuracy. For example, one empirical research measures two groups of people with positive intention (i.e., inclined actors) and negative intention (i.e., disinclined abstainers) on different scenarios and conclude that the significant contrast is to act as their designed intentions (McBroom & Reid, 1992; Orbell & Sheeran, 1998). The gap can be explained by different changes, either on scale correspondence, measurement error, different elements and so on (Sheeran., 2005).

Intentions are predicted by diverse antecedents which depend on the theory and the scenario.

The privacy paradox theory believes otherwise as well, behavior attitudes directly affect intentions which advance a particular gap among individual's intention and behavior attitude towards their actual behavior (Joinson et al., 2010, Pötzsch, 2009, Tsai et al., 2006). While people claim to be concerned over privacy, it appears that they freely provide personal data.

In privacy context, intentions are shaped by attitudes, subjective norm and perceived behavioral control (Ajzen 1985). Moreover, another research confirms that intentions are formed independently through factors such as behavioral routine (Ouellette and Wood, 1998).

If various investigations have been made to clarify the attitude-behavior gap in the recent literature (Michaelidou & Hassan, 2014, Ackermann and Palmer, 2014, Iweala et al., 2019, Padel and Foster, 2005, Valkila and Saari, 2013, Vermeir and Verbeke, 2008, Zhou et al., 2013),

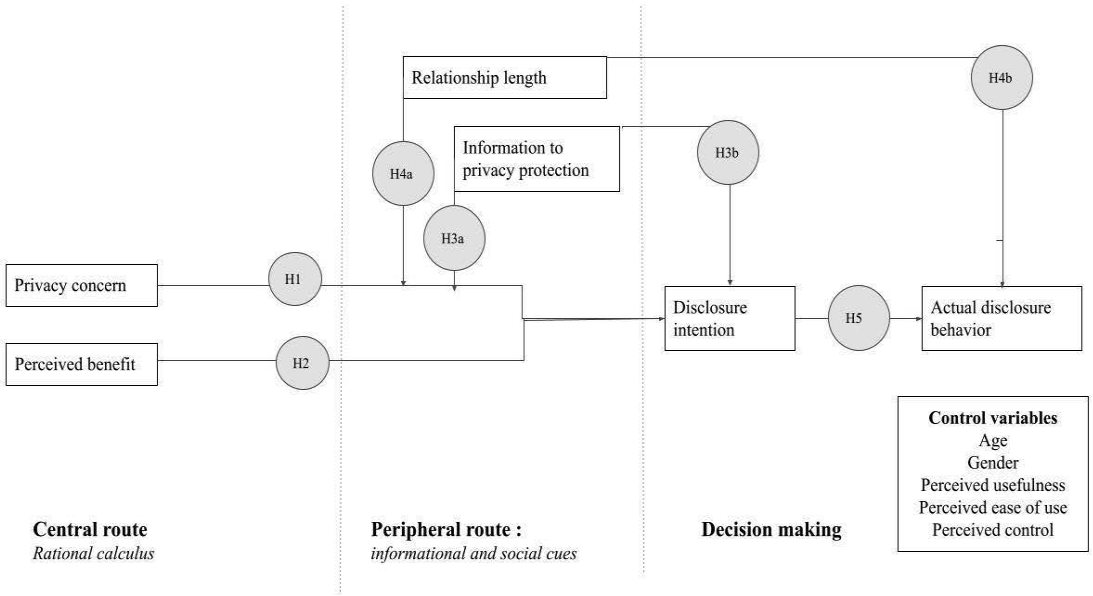
works exploring ways to analyze intention-behavior gaps in disclosure are limited (Adjerid and all., 2018; Hassan and all., 2016; Norberg and all., 2007) and even less than once we integrate the decision making process. Likewise, we can find in the appendix 3, the discrepancy analysis in disclosure behavior made on different contexts.

To define this gap in our study, we crossed theory with ELM to understand the role of the decision-making process on hypothetical to actual choice.

3. HYPOTHESIS

Based on the privacy calculus and privacy paradox, our study integrates three main factors: privacy concern, benefit perception and heuristic factors that influence disclosure intention and actual behavior and integrate them to the ELM. As mentioned previously in the literature review, the heuristic cues introduce the relationship length and information to privacy protection. Then, we first hypothesize that factors in central route and peripheral route are directly associated with information disclosure intention and actual disclosure behavior respectively. We also suggest that heuristics cues moderate the relationships between the factors in central path and information disclosure intention. Concretely, we assume that being informed about AIA's privacy protection weakens the negative relationship between privacy concern and disclosure intention. In contrast, this latter relationship became stronger in a long-term relationship with AIA. Figure 1 shows the proposed hypotheses, which we justify here after.

Figure 1: Revised model of crossing theories between ELM and privacy paradox



3.1. Central route

The strong desire for perceived benefits will put the user's privacy at stake, as personalized services for Smart Personal Assistant (SPA) require a certain degree of personal data provided by users. For instance, users who command SPA to give information about traffic congestion lead smart personal assistant (SPA) to request users' location in the process. If they oppose sharing the latter information, it will not be favorable for the device's task efficiency nor the users' needs. This dilemma has always been reviewed in past works (Lahlou et al., 2005; Dinev et al., 2006; Wu et al., 2018) and required to weigh the risks and benefits in a thoughtful way. In the AI context, our study will then indicate privacy concerns and benefit perception as main factors in the central route.

Recent research reveals the rise of smart personal assistant (SPA) user's issues over their privacy (Abdi, N., & M. Ramokapane, K. 2019; Lau et al., 2018). As a matter of fact, these devices are passive listeners who hear everything around the users. Results from recent empirical work show how reviewers expressed their concern whether in the amount, range or type of data collected by SPA (Fruchter et al., 2018). More importantly, other studies argue that privacy concerns influence disclosure intention (Wang et al., 2019, Zlatolas, Welzer, Heričko and Hölbl (2015). However, this influence lead people to withhold their data. To be specific, individuals are reluctant to share their personal information due to perceived risks such as privacy harms or misused of the data by SPA (Naeini et al. 2017).

Despite these concerns, these technological devices also raise various advantages, such as providing personalized information, online purchases, entertainment, or control over smart home devices (Cha et., 2021). In 2020, music stream service and research information became the most frequent use in the US (Statistica, 2020) (Appendix 5). The belief to experience personalized features can be a prior motive for users to give away personal information. Besides, previous studies confirm how strong individual's preferences for smart personal assistant's (i.e., SPA) innovation services influence self-disclosure intention (Lee et al., 2011).

Furthermore, prior research states rational factors significantly influence the behavioral intention compared to the actual behavior (Dinev and Hart, 2006). According to the privacy paradox model, actual behaviors usually have hypothetical future plan (i.e., intentions) attached to them (Barth & de Jong., 2017). However, intention is not sufficient impetus for the actual

action (Bagozzi, 1992). Typically, the difference relies on their contextual disposition. Researcher states that hypothetical choices do not generate drawbacks, and require some cognitive resources compared to actual decision which is known as instantaneous, subject to high risks, and followed by emotional properties (Kang et al., 2011). Hence, intention is a hypothetical choice for future plan while actual behavior is applied to a real-life context. On one side, rational calculus in privacy aims for optimal solutions for future solutions (Kehr and al.,2013) and required in depth evaluation for the decision-making process (Foster & Young., 2001). Thus, the strong association between intention and rational factors can be interpreted as their common ability for predicting upcoming decisions. On the other hand, when people are exposed to the actual future, researchers argue that the outcome is presumed to diverge as preference might change over time (Acquisti & Grossklags., 2003). Preference such as benefit perceived in disclosure is time-inconsistent which explains disparity between actual behavior and attitudes set with rational decision process (Kokolakis., 2017). Similarly, the theoretical concern individuals claim over their data are rarely effective when times required to actually protect them (Joinson et al., 2010).

Therefore, to measure individual's influence on their privacy concern and benefits in their intent to disclose personal information, the following hypothesis are made:

- H1: individual's privacy concerns over smart personal assistants have negative influence on information disclosure intention compared to the actual disclosure.
- H2: individual's perceived benefits over smart personal assistants have positive effect on information disclosure intention compared to the actual disclosure.

3.2. Peripheral route

People use heuristic process while relying on cues to minimize cognitive effort towards message processing. Nonetheless, the sense of judgment may not be accurate (Chaiken, 1980). Recent work suggests social heuristic cues and informational cues as two main elements of the peripheral route to influence self-disclosure in an online environment (Adjerid et al., 2018; Wang et al., 2019). Besides, these cues may generate approval or refusal to the perceived message (Mondak J., 1993). Following the literature mentioned previously, we establish that the information to AIA's privacy protection (i.e., informational cue) and the relationship length (i.e., social cue) are factors in the peripheral route. Past empirical work argues how specific heuristic cues, which depend on low effort cognition, are direct predictors to actual behavior

(Norberg and all., 2007). If the ELM model shows that both central cues and heuristic cues influence behavioral intentions that would then influence actual behavior, we argue that this is not the case. In fact, the crossing theories engage beyond the original privacy paradox model. We can find the original model of the privacy paradox in appendix 1 and 2.

As the dual process could operate simultaneously or independently, we argue that heuristic cues are not predictive of behavioral intention but may operate directly in actual disclosure which depend on the context. The following discussion clarifies our positions on the two peripheral cues and their influence on actual disclosure.

Information to AIA's privacy protection

One study posited how privacy notices significantly influence self-disclosure (Adjerid, I., and al., 2013). Individuals who are more knowledgeable about the companies' privacy protection have a higher tendency to share personal information. Some researchers reveal that online users value privacy notices to feel a sense of security and increase their feeling of being protected (Awad & Krishnan, 2006; Milne & Culnan, 2004; Tsai et al., 2011), as a result enhancing disclosure behavior (Hui, Teo, & Lee, 2007).

Therefore, researchers stated privacy policy among the direct predictor to information disclosure intention (Zlatolas et al., 2015). Individuals are inclined to share their personal information if they have a reference point about the use of their data. We believe this pre-existing information infer an intention attempt to self-disclose but still far to do so, as information are likely to change. Thus, previous work mentions how information to privacy protection strongly affects hypothetical choice than actual behavior to disclosure (Adjerid, and al., (2018). The following hypothesis is arranged:

H3a: Individual's information to privacy protection of smart personal assistant positively influences information disclosure intention compared to the actual disclosure.

Subsequently, companies behind those SPA are subject to some issues over security and privacy matter. For example, studies found some speech recognition vulnerabilities to Amazon on SPA's capacity (Haack et al, 2017) and others news mentioned potential massive audio surveillance from the workers in Amazon (Picchi, 2019) which the latter argues that they do not possess the right access to their user's personal perceptible information (BBC news, 2019). Even so, several studies focused more on the influence of concern over security and privacy compared to security and data policy information towards AIA. Recent research suggests that users have inaccurate thoughts on SPA data processing, storage, and learning (Abdi, N., & M.

Ramokapane, K., 2019). Therefore, providing fair information and firm's transparency to the latter usage may reduce their privacy concerns (Bleier, 2020). Moreover, Culnan and Armstrong (1999) posited that the use of right information processed by firms can raise trust and decrease privacy concerns and perceived risks of disclosure to consumers. In the online environment, the presence of privacy seals has been found to have a positive effect on the perception of trust (Rifon et al. 2005). The information of the individual on SPA's privacy protection will likely moderate the effect on disclosure decision-making by lessening the discomfort to share information.

Thus, the following hypothesis is built:

H3b: Individual's information to privacy protection of smart personal assistant will decrease the negative relationship between privacy concerns and self-disclosure intention.

Relationship length towards AIA

Researchers have introduced the role of relationship length in different theories and contexts such as social influence (Robert Cialdini,1984) or social exchange theory (Palmatier et al., 2006), which is initiated to be part of the social cues. Subsequently, self-disclosure acts as an essential phase of the social relationship (Greene et al., 2006). According to social penetration theory, as the relationship develops, the breadth and depth of self-disclosure increase (Altman and Taylor, 1973). This theory gives a prior approach on the relationship between self-disclosure, the relationship length and the level of closeness revealed as a relational consequence. The more time we spend with others, the more likely we are to share deeper information. Despite Taylor and Altman applying this theory between human-to-human interaction, compared to the traditional technology, AIA's smart features are acknowledged in the literature as being anthropomorphic (i.e., human-like) regarding its user-friendly service, interactiveness and professionalism. Nonetheless, self-disclosure is considered as more salient in computer-mediated communication compared to face-to-face contact. Other research even indicates the interpersonal relation between individuals and text-based computers (Moon and Nass, 2000) and the gradual stage of the depth of the information to be disclosed once following interpersonal communication through the years (Fehr, E. & Gächter, S, 2000). Recent work related to the actual behavioral disclosure and relationship development on IoT have also been investigated and confirmed their strong association (Li. Z and Pei-Luen, 2019).

Moreover, researchers mention how intimacy is defined by different key aspects and among them, are depth and breadth of information exchanged and length of relationship (Walster &

Berscheid., 1978). The literature posits that as two parties became intimate, they disclose more information at a deep level. In contrast, as the relationship changes from highly intimate to nonintimate, self-disclosure should reduce in breadth (Tolstedt & Stokes., 1984). This process is called social depenetration (Altman & Taylor., 1973) and is considered as the reversal process in social penetration theory. The reason is that while the relationship is gradually dissolving, a large amount of negative judgments, evaluations and even feelings are involved in the communication (Tolstedt & Stokes.,1984). More importantly, researchers (Grayson & Ambler., 1999) argue how long-term relationship lessen the involvement of use from a marketing service perspective. (Moorman and al., 1986) explain that this low involvement is caused by lower valuable perception and predictable aspects on the service as time goes by. Thus, with a long-term relationship, users will perceive less desirability to the services and later decrease interactions.

Besides, the behavioral literature suggests that privacy judgments can be relative in nature (Egelman et al. 2013). Researcher posits that consumers might compare their (current) situation to past events or habituation (Gable & Reis., 1999). Thus, research advanced that time fluctuation conveys about relationship processes in everyday activity (Gable & Reis., 1999). Therefore, we believe that relational behavior is common to real life decisions and (Ross, 1989; Sprecher, 1999) posits how time period gave insights to the actual changes in people's choices. Accordingly, several studies proposed that the influence of such heuristic factor may be even more important in actual decision context compared to hypothetical choices (Acquisti et al. 2012; Brandimarte et al. 2012; Egelman et al. 2013; John et al. 2011). Then, we establish that relationship length, as a behavioral (i.e., heuristic) factor is more salient to actual disclosure compared to intention (Acquisti et al. 2012; Brandimarte et al. 2013; John et al. 2011).

Furthermore, we assume that the more lasting the relationship between the users and AIA will be, lower the propensity to actually share personal information in parallel to their intention. Hence, we establish the following hypothesis:

H4a: Long term relationships with the AIA have a negative impact on an individual's actual information disclosure compared to disclosure intention.

Scholars argue that positive and negative feelings in social relationship evolve over time (Blau, 1964; Gouldner, 1960; Homans, 1950). In this regard, researchers also advanced that social relationships initiate either reciprocated trust or distrust (Lewicki et al., 1998).

Thus, we assess that trust or distrust are consequential attributes developed through a mature stage of the relationship. Accordingly, low trust levels are relative to high distrust levels and inversely (Marsh & Dibben, 2005). Besides, past privacy work indicates the salient connection of distrust and the privacy concern (Scheen., 2014). Hence, relative to the definition of distrust (Lewicki et al., 1998), the concern over privacy reveals a sense of fear and risk that another may perform negative action towards personal data.

Furthermore, based on the AIA context, recent research confirmed that in a long relationship with AIA, people are subject to an important identity threat, resulting to privacy concerns (Uysal, E., Alavi, S., & Bezençon, V., 2022). In this range, the downsides of the relationship became more apparent in a long duration and as the uncertainty mentioned above is even more triggered compared to short duration. Researchers argues that individuals process great amount of information within a long-lasting relationship in contrast to the early ones (Dagger & Gibbs., 2008).

Based on these references, we believe that the negative relationship value accumulated over time might dampen even more the trust (Brandimarte et al., 2012) and heighten distrust, as reinforcing privacy concern and initiate reservation towards disclosure.

Despite that work related to the relationship length over the disclosure decision-making is scarce, our analysis believes that relationship length act as a moderator to the relationship between privacy concern and self-disclosure intention.

Therefore, our hypothesis carried the following statement:

H4b: Long (.vs short) term relationship with the AIA strengthens (.vs weaken) the negative connection between privacy concern and the disclosure intention.

Intention-Behavior relationship

Measuring those previous antecedents allow a better comprehension of factors responsible for intention-behavior discrepancies in general. Several studies used to measure privacy attitudes to determine behavior intention in a rational process and neglect the actual outcome could be slightly different (Dinev et al., 2015). Accordingly, past works confirmed how intention is assumed to be prior predictor of behavior.

Following the privacy paradox theory (Norberg, 2007) and applied to an AIA context, we posit that intention predict the actual behavioral disclosure. We then expect to confirm this argument by building the following hypothesis:

H5: Individuals intention to disclose information to AIA positively influence their actual disclosure behavior.

4. METHODOLOGY

4.1. Research settings and survey design

This research uses a quantitative method. We refer to previous research for consistency in our methodology (Norberg and al., 2007; Wang and al., 2019) and arrange an online survey. Moreover, our participants may appear unmotivated and burdened with an experimental approach. Then, a pilot test was conducted to verify clarity and validity of the items provided. 7 individuals with different demographics backgrounds were requested to evaluate the items regarding the form, semantics, and understanding of the survey.

Finally, the study used Qualtrics (Qualtrics, 2022) as a professional tool to frame the questionnaire. Later, a link was sent to the respondents via social media (Facebook and LinkedIn) in a community group research study and via university students mailing. We can find the list of the survey distribution channel in appendix 6.

4.2. Measures

Main variables

We measure the following variables in multiple item scales: privacy concern, perceived benefits, relationship length, information to privacy protection, self-disclosure intention and actual disclosure. All items used 7-point scale (1=Strongly disagree to 7= Strongly agree) measurements except for relationship length and actual disclosure intention.

We asked the users the duration of use of their smart speaker or smart virtual assistant in a single choice question. Regarding the actual behavioral disclosure, we used 5 points scales (1=never to 5=very often) based on how often they have done the behavior. This measurement scale is based on the theory of planned behavior questionnaire (Ajzen, 2002).

For AIA non-users, we prepare a similar set of questions aligned with the actual behavior but by replacing the focal object, i.e., AIA to online context.

The list of presentation order and measurement items of main variables along with their sources are shown in appendix 4.

Control variables

We also integrated control variables to ensure balance in our study, which are based on technology acceptance, demographics characteristics and control perception.

Firstly, we assess two variables from the technology Adoption Model (TAM) (Davis, 1989), which integrate perceived usefulness and perceived ease of use in explaining the acceptance of such cutting-edge technology (i.e., IPA). Based on different definition applied in the literature, we define perceived ease of use as an individual's perception on the level of effort set on certain technological mechanisms practices (Burton-Jones and Hubona, 2005; Venkatesh, 2000). Researchers also argue that if the technology is perceived easy to use, there will be more exposure and less barriers to start sharing personal information (Davis, 1989; Khan, 2020).

Perceived usefulness considered individual's perception on a system's effectiveness level once used (Davis, 1989). This perception is also considered as the main predictor for technology acceptance which have been proved in one AIA contextual work (Uelsen., 2021). Perceived usefulness was also proven to significantly predict self-disclosure (Beldad, 2015; Beuker, 2016).

Secondly, we included perceived control over data disclosure. The theory of planned behavior argues how perceived behavior control is crucial determinant to the gap between intention to actual behavior (Ajzen, 2002). Moreover, empirical work stated that having control over privacy is proven to strongly impact self-disclosure (Shih, 2012). For an individual to perform the behavior, that person must have control over it.

Lastly, we added demographics variables to the study. Other research posits that age is salient in the purpose of smart devices use (Garg et al., 2020). More importantly, age influence the privacy decision (Chakraborty et al., 2013). Recent study has proven that older generations are less adamant to share their personal information online compared to younger ones (Kim et al., 2019). Aside, we also assess gender as control variable. Previous study shows that gender plays a salient role in disclosure behavior (Yu, T., 2014). For instance, women claimed to be more concern towards their privacy when sharing information to smart personal assistant (Cao and Wang, 2022). Furthermore, there is strong evidence that women are the one who disclosed more personal information compared to men (Cozby 1973; Yu, 2014). Thus, we expect to use those control variables over the regressions analysis that will be operated towards the main variables.

4.3. Participants

The survey distribution lasts for two weeks from May 25 to June 6, 2022. A total of 153 responses were collected. Nonetheless, we suppressed invalid data and missing responses. As far as our knowledge, the missing data are generated because some people do not seek to continue and decided to stop in the middle. As we purposely did provide insurance for any misused information, this may have an impact on the respondent's trust and willingness information disclosure. Furthermore, we indicate that the participants may pursue to answer later or leave if not comfortable with the questionnaire and therefore, leading to some blank responses. We also observe duplicate IP errors which generate these blank responses. As a result, a total of 109 questionnaires are gathered.

5. ANALYSIS/RESULTS

5.1. Statistical analysis

We use SPSS (IBM, 2015) and SPSS Amos software (IBM, 2019) and conduct two steps in our measurements. Firstly, we assess the reliability and validity of all the constructs. Then, we test the relationships of all the variables through a regression analysis.
Therefore, (Fornell and Larcker, 1981)'s explain that the scale reliability can be measured by determining the average variance extracted (AVE) and composite reliability.
Then, we measure the reliability of the items and scales with the 6 main factors, which are: privacy concern, perceived benefit, information to privacy protection, intention disclosure and actual disclosure with their respective items and established scales. Relationship length is not included in the measurement as reliability cannot be assessed with single item measures. The list of the items is provided in table 3 and appendix 4.

Then, we investigate the convergence and discriminant validity of the multi-item's scales. (Hair et al., 2020) suggest that convergent validities are conform if the loadings of items and their respective constructs are above 0.55. Then, discriminant validity can be assessed if the square roots of the AVEs of any latent variables are larger than the correlations shared between the latent variable and other latent variables (Barclay et al., 1995).

We will also assess a correlation model to investigate potential association and prevent multicollinearity in the measurement.
Subsequently, to test privacy concern-intention disclosure, privacy concern-actual disclosure(H1), perceived benefit-intention disclosure, perceived benefit-actual disclosure (H2), information to privacy protection-intention disclosure, information to privacy protection-actual disclosure (H3a), relationship length-intention disclosure, information to privacy protection-actual disclosure (H4a), intention disclosure-actual disclosure (H5) relationships were assessed using a regression analysis as mentioned previously. We include the control variables in the analysis (gender, age, perceived usefulness, perceived ease of use, perceived control). Then, we operationalize two main dependents variables: intention disclosure and actual disclosure. Each variable was tested separately because when tested all together, they exhibit covariances, especially perceived benefit, information to privacy protection and

relationship length (Appendix 13). (Hair et al., 1998) justify that if two measures are likely to covary, even if they are different, then the measures can be regressed separately.
Additionally, we also measured the effect of relationship length and information to privacy protection on the relation between privacy concern and intention disclosure (H3b), (H4b). Table 4 presents our regression analysis along its results.

5.2. Results

Approximately 59,6% are found to use smart personal assistant or smart speaker and 40,4% do not use it. Amongst the respondents, 62,5% and 37.5% percent of the respondents are female users and non-users respectively, and 28,4% percent are male respondents and more than half of them used AIA. Finally, the remaining respondents are unwilling to disclose gender information. Moreover, we did not find any respondents between 30 to 40 years old and the number of people who are above 40 years old of age is scarce. Instead, the majority (97,3%) of the participants are between 19 to 28 years old, with 62% are smart virtual assistants' users: This result corresponds with the recent statistic on the average age of smart speaker owners conducted in 2019 (Kinsella, 2019) and seen in appendix 7. As a general information, our finding also posits how Siri dominates among adult Gen Z (Appendix 8).

The demographic characteristics of the respondents are reported in Table 1 below.

Table 1: Demographics characteristic of the respondents (109)

Category	**Item**	**N**	**Percentage (%)**	**Users N (%)**	**Non-users N (%)**
Gender	Male	31	28,4	17(54.8)	14(45.2)
	Female	72	66,1	45(37.5)	72(62.5)
	Unwilling to disclose	6	5,5	3(50)	3(50)
Age	18 years old and below	2	1,8	2(100)	0

Category	Item	N	Percentage (%)	Users N (%)	Non-users N (%)
Age	19-40 years old	106	97,3	62(58.5)	44(41.5)
	over 41 years old	1	0,9	1(100)	0
			TOTAL	65 (59,6)	44 (40,4)

Reliability and validity

Following analysis of scales measurements, our results show that we have sufficient reliable, convergent and discriminant validities. The results provided in table 2 indicate that all the scales we operated in this model are conform to reliabilities, with an average variance extracted (AVE) above the minimum recommended value of 0.50, as well as a composite reliability (CR) which is above 0.7. Although there are two exceptions, which was slightly below the AVE threshold (AVE = 0.45 for actual disclosure and AVE =0.44 for intention disclosure) but admit higher composite reliability above 0.7 (CR=0,80 for actual disclosure and CR=0,75 for intention disclosure), then we conclude that the constructs' validities are adequate as suggested by (Fornell & Larcker, 1981). Regarding the convergent validities, the loading of each item and their respective constructs are higher than 0.55 and can be seen in table 2 below. Furthermore, the results in appendix 12 show that the square root of AVEs of each construct is strongly related to its oneself compared to other construct, which suggest an acceptable discriminant validity.

Table 2: List of measurement of items and scales evaluation for main variables

Construct	Item	Loading	M		V	AVE	CR
1.Privacy concern	PC1: It is very important to me that I am knowledgeable about how my personal information will be used.	0,752	5,315		2,42	0,65	0,85
	PC2: I am worried Smart Speaker/Smart Personal Assistant will share my personal information with other firms.	0,857					
	PC3: It bothers me to give my personal information to Smart Speaker/Smart Personal Assistant.	0,806					
2.Perceived benefit	PB1: Smart Speaker/Smart Personal Assistant can provide me with personalized services.	0,708	5,636	2,4	0,52	0,77	
	PB2: Smart Speaker/Smart Personal Assistant ensures productivity to my mundane tasks.	0,797					
	PB3: Smart Speaker/Smart Personal Assistant can provide me with entertainment.	0,659					
3.Intention disclosure	how easily would you consider giving the following information? ID1: Your annual income	0,556	3,156	3,68	0,44	0,75	
	ID2: Your sexual orientation	0,798					
	ID3: Your address	0,699					
	ID4: Your phone number	0,58					
4.Actual disclosure	How often AD1: have you disclosed your credit card information for Smart Virtual Assistant's purchase feature? /For online purchase?	0,65	2,473	1,94	0,45	0,81	

Construct	Item	Loading	M	V	AVE	CR
4.Actual disclosure	AD2…have you updated your address location to be used by Smart Virtual Assistant? /To be displayed online?	0,699				
	AD3: …have you updated your phone number to be used by Smart Virtual Assistant? / To be displayed online?	0,693				
	AD4: did you allow your personal photos to be used by Smart Virtual Assistant? / To be displayed online?	0,75				
	AC5: …did you delete your information search history stored by your Smart Virtual assistant? /…did you delete your online search history?	0,564				
5.Information to privacy protection	IPP1: I am informed how my personal information will be used by Smart Speaker/smart virtual assistant.	0,905	3,651	3,27	0,81	0,93
	IPP2: I am informed how my personal information will be stored by Smart Speaker/smart virtual assistant.	0,903				
	IPP3: I am informed how my personal information will be protected by Smart Speaker/smart virtual assistant.	0,908				
6.Relationship Length	RL: How long have you used a Smart Speaker/Smart Personal Assistant?	-	-		-	-

Note: PC, Privacy concern; PB, Perceived benefit; ID, Intention disclosure; AD, Actual disclosure; IPP, Information to Privacy Protection; RL, Relationship Length; M, mean of each construct; V, Variance of each construct; AVE, Average Variance extracted, CR, Composite reliability. CR >0.7; AVE> 0.5; **α**>0.7 or 0.5 (for less than 10 items).

Correlations

Table 3 shows the correlations among the variables. Privacy concern and intention disclosure are significantly and negatively correlated (b=-.350, p<.001). Perceived benefit is significantly positively associated with intention disclosure (b=.196, p<.05).

Moreover, we perceived that individuals' actual disclosure information and relationship length are significantly negatively correlated (b=-.368, p<.001). Besides, the mean of the relationship length (M=2,52) suggests that the respondents used AIA during a term period between 1 to 2 years. In contrast, people who are informed about AIA's privacy protection admit a significant association with the intention disclosure (b=.328, p<.001).

Table 3: Correlations of all the variables

Variables	Mean	SD	1	2	3	4	5	6	7	8	9	10	11
1.Privacy Concern	5,31	1,29	-										
2.Perceived Benefit	5,64	1,14	-,043										
3.Intention Disclosure	3,16	1,43	-,35**	,196*									
4.Actual Disclosure	2,47	0,94	-,121	-,013	,243*								
5.Informa-tion to Privacy Protection	3,65	1,66	-,118	,173	,328**	,061							
6.Relation-ship Length	2,52	1,58	-,171	,095	,014	-,36**	0,077						
7.Perceived ease of use	4,53	1,30	,058	,238*	0,04	-,242*	0,154	0,18					
8.Perceived usefulness	4,96	1,32	-,119	,241*	,067	-,133	,198*	0,16	,378**				
9.Perceived Control	3,53	1,36	-,128	,186	,267**	0,084	,306**	,080	,104	,182			
10.Age	20,9	3,30	,202*	,154	-,110	-,154	-,065	,077	-,026	,080	,022	-	-
11.Gender	1,77	0,53	,012	,083	-,058	-,039	,013	,033	-,149	-,065	-,097	,004	-

Notes: SD, Standard Deviation; PC, Privacy Concern; PB, Perceived benefit; ID, Intention disclosure; AD, Actual disclosure; RL, Relationship length; IPP, Information to Privacy Protection. Off-diagonal elements are the correlations among constructs. *p=<0.05; **p=<0.01; ***p=<0.001.

Regression analysis

Table 4 represents the results of the regression mentioned in the statistical analysis.

As mentioned in our hypothesis, privacy concern towards AIA is found to negatively affect an individual's intent to disclose information (b=-0.349, p<.001) and do not have any influence on actual disclosure (b=-0.052, p=.456). Subsequently, perceived benefit has a moderate but positive influence on intention disclosure (b=0.244, p<0.05) without the control variables applied but appears to be less important once the latter are included (b=0.235, p=0.063).

Moreover, the effect of perceived benefit appears to be less salient towards actual disclosure (b=0.11, p=0.437). Therefore, H1 is supported as the participants who are concerned over their privacy had less intent to disclose their information, but not salient enough to affect their actual behavior to disclosure. In contrast, H2 is rejected as the result for perceived benefit-intention disclosure relationship was found to be not significant.

Then, relationship length's effect on actual disclosure was admitted being significant and negative (b=-0.195, p<0.001) compared to intention disclosure (b=-0.001, p=0.429). Moreover, being informed about privacy protection positively influence the intent to share information (b=0.233, p<0.01) and appear to be less salient towards actual behavioral disclosure (b=0.042, p=0.458). Thus, H4a and H3a are supported.

Regarding the moderator's effects, information to privacy protection and the relationship length has no significant effect on the relation between privacy concern and intention disclosure (b=0.234, p=0.449), (b=-0,182, p=0.654). We also reduce the covariance between relationship length and privacy concern, but the result remains the same. Then, H3b, H4b are rejected.

Our last analysis implied the direct association between intention and actual behavior. Our finding shows that people's intention to disclose information positively influence actual disclosure behavior (b=0.148, p<0.05). However, the power of the intention to explain actual disclosure is quite low (R^2 = 0,15). Accordingly, appendix 11 shows that AIA users' intentions to share their personal data appear to be salient when asking their actual behavior disclosure responses. Thus, H5 is supported.

Table 4: Regression analysis

IV	DV	Full model			Model w/out control variables		
		R^2	Coef(SE)	p	R^2	Coef(SE)	p
Privacy Concern (PC) H1	Intention disclosure	0,177	-0,349 (0,104)	0,001***	0,122	-0,387 (0,100)	0,000***
Perceived benefit (PB) H2	Intention disclosure	0,117	0,235 (0,125)	0,063	0,038	0,244 (0,118)	0,042*
Information to Privacy protection (IPP) H3a	Intention disclosure	0,150	0,233 (0,084)	0,007**	0,108	0,282 (0,078)	0,001***
Relationship Length (RL)	Intention disclosure	0,086	-0,001 (0,088)	0,429	0,000	0,012 (0,087)	0,367
Privacy Concern (PC)	Actual disclosure	0,109	-0,052 (0,071)	0,466	0,015	-0,089 (0,070)	0,209
Perceived benefit (PB)	Actual disclosure	0,109	0,065 (0,083)	0,437	0,000	-0,010 (0,080)	0,896
Information to privacy protection (IPP)	Actual disclosure	0,109	0,042 (0,057)	0,458	0,004	0,035 (0,055)	0,526
Relationship Length (RL) H4a	Actual disclosure	0,205	-0,195 (0,054)	0,001***	0,136	-0,220 (0,054)	0,000***
Intention disclosure H5	Intention disclosure	0,150	0,148 (0,063)	0,021*	0,059	0,161 (0,62)	0,011*
Main effect of the moderators							
PC*RL H4b	Intention disclosure	0,182	0,017 (0,060)	0,78	0,126	0,026 (0,058)	0,654
PC*IPP H3b	Intention disclosure	0,234	0,023 (0,048)	0,637	0,210	0,036 (0,049)	0,449

Notes: PC, Privacy Concern; PB, Perceived benefit; RL, Relationship length; IPP, Information to Privacy Protection. Coef =Standardized coefficients, SE=standard error. Hypothesis are written in bold. *p=<0.05; **p=<0.01; ***p=<0.001 (two tailed). **(H1, H2, H3a, H4a, H5 are supported, and H3b and 4b is rejected).**

5.3. Robustness check

To prevent common method bias in our analysis, we applied a Harman single factor test. We observed that the total variance extracted is below 50%, equivalent to 12,49%. Likewise, this result indicated that common method variance (CMV) was not a major concern. We also tested all the variables conjointly through a multiple linear regression with 4 structural models, aside the multicollinearity and covariance (Appendix 13), the results are relatively the same as when all the variables are tested separately (Appendix 12).

To determine our model's accuracy, we also bootstrapped the regression model, and the results remained stable as seen in appendix 10.

6. DISCUSSION

The results of the study confirm that every individual's rational thinking brings an impact on intention disclosure to AIA. However, the trade-off is far away to be expected. People's concern over their privacy remain to affect sharing decision (H1). However, compared to previous studies which demonstrated that perceived benefit enhances self-disclosure, the result of this study shows otherwise (H2). This disparity is partly due to the multicollinearity (Shrestha, 2020; Steyerberg, 2016) between the perceived ease of use, perceived usefulness of the AIA and the benefits users and non-users recognized, which lessen the power of the predictor. While reducing the effect of the multicollinearity by standardizing the variables, the result shows that perceived benefit have a significant impact on self-disclosure intention (Appendix 9). This result maintains the rational calculus theory mentioned in the literature.

We also observed the strong influence on heuristic cues on self-disclosure. Our findings suggest how well information to privacy protection influences directly self-disclosure intention (H3a). Furthermore, longer duration in the relationship admits affecting the way people surrender their personal data (H4a). However, these heuristic cues do not moderate the relationship between privacy concern and intention disclosure (H3b, H4b).

Furthermore, our findings perceived that intention predict actual behavior in disclosure (H5). People are willing to share personal information to AIA based on their inner intentions, which confirm the past literature (H5). However, the result demonstrate that intention does not explain fully actual disclosure. As far as our knowledge, we interpret the previous antecedents are important contributors for such variations, following by the scale imbalance.

7. CONCLUSION

Contributions

This research aims to understand a particular behavior confirmed by different works over the years but rather in a different setting. Through different research, we believe that people's disclosure behavior is affected by some stimuli. Particularly, those factors implied the cognitive cues and the heuristic or bias route. The purpose of our study is to confirm whether the latter is also applied in an AIA conceptual base.

The privacy concern-benefit assessment factors are predominant in disclosure decision making towards AIA. We suggest that future research might be directed toward discerning the effect of rational calculus on disclosing information to AIA in more experimental approach and manipulate the elements being trade. Aside the risk-benefit attributes, we believe that trust can be an important factor to investigate self-disclosure. Trust can be observed as a rational factor in privacy decision making. In the online environment, users with a higher trust are more likely to share personal information as trust lessen the risk (Frost-Arnold, K., 2012; Wu et al., 2012).

Subsequently, we confirm that there is a significant discrepancy between intention and actual disclosure. Otherwise, it appears that this dichotomy overturned the privacy paradox theory. Except for the cognitive factors, heuristic cues are main determinants by explaining this gap in the realm of this high technology. The relational dynamics are at stake in a longer relationship and privacy concern pressured even more the users. In contrast, the informational cue reveals a positive effect on self-disclosure intention.

Following these investigations, we contribute of two theoretical key points in the literature. Firstly, our research extends to all artificial intelligence assistants rather than one branded AIA (e.g., Alexa, Siri, Google, and so on…) and can offer great insights on specific research in the future. Secondly, the matter of dual processes in privacy remained a question in past research but few have investigated those factors' influence on intended and actual privacy behavior all together in an AIA environment. Then, our study helps to extend the privacy paradox literature (Barth, 2017; Norberg, 2007) by investigating the gap and its underlying mechanism's influence.

Limitations

Despite these contributions, our research is subject to some limits. Our first limitation is related to the measurements. Despite that some of the survey questions are from reliable sources, our study required to not be fully described by different privacy antecedents nor all the items are adapted from sources as the AIA study in privacy is scarce and complex compared to other scenarios. We also suggest that for future empirical work, the scale need an adjustment for consistency.

Our second constraint is due to the amount of time and resources, we adopted an empirical approach suitable for our study and helps to highlight previous findings. This method is not the most ideal as determining the actual behavior was not an easy task. Therefore, we assess past behavior in disclosure to be relevant on evaluating the individual's complexity of making decision. Whereas future research can develop further understanding of this process by adopting a more practical method and with a large sample size to complement our findings.

In addition, we find that heuristic cues are difficult to determine and to measure. They are considered as frugal and might require a specific situation to determine their power's effect. Future researchers could determine different heuristic cues that influence privacy decision-making in general context.

Moreover, social factors towards AIA's self-disclosure were not fully explored in past works. Relationship length is strongly associated with relationship closeness and interaction frequency. Despite our study did not elaborate more on other social cues and its potential positive effect, future research can investigate the relational effect on these attributes in self disclosure and enrich our findings.

Away from the self-disclosure subject, users might develop feelings of closeness with AIA because of its human-like feature. It will be interesting to deepen the research if those feelings motivate the users to engage more and to commit more to the brand. Future research could determine if this connection elevates customer engagement, and later loyalty. Therefore, it may help on companies' marketing plans and to improve AIA's personalized services.

Recommendation for managerial implications

Based on these results, we present some recommendations for managerial implications.

First, companies behind AIA should improve the communication of their privacy protection technology which will reduce their future and former costumer's concerns. Therefore, smart

virtual assistant service providers should thoroughly notify costumers regarding their data processing, collection, storage, or use and brief them if any changes are made. Furthermore, costumers who are well informed about privacy policy will feel more at ease to share information. They should also allow smart speaker to only collect relevant data and construct preventive measures for any threats.

Second, companies should allow AIA to enhance valuable services in accordance with the needs of the potential target and avoid irrelevant promotions. Managers must focus on perceived beneficial factors, like hedonistic or technical motivations for the consumers to be attracted and use their AIA more. This would translate to competitive advantage in a realm where different brands for smart virtual assistants (e.g., Alexa, Google, Siri, and so on.) exude presence.

Third, companies are advised to operate a costumer's engagement strategies to sustain the relationship between AIA and the users but in a way to ensure active interaction and relational bond. Service providers should enable to nurture the relationship and ensure self-efficacy without trespassing the boundaries of privacy users might have.

8. LIST OF REFERENCES

Abdi, N., & M. Ramokapane, K. (2019). More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. *USENIX Symposium on Usable Privacy and Security (SOUPS)*, 11–13.

Abdi, N., Zhan, X., Ramokapane, K. M., & Such, J. (2021). Privacy Norms for Smart Home Personal Assistants. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3411764.3445122.

Acquisti, A., & Grossklags, J. (2003). Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior. *2nd Annual Workshops on Economics and Information Security*, 1–27.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy Magazine*, *3*(1), 26–33. https://doi.org/10.1109/msp.2005.22.

Acquisti, A., John, L. K., and Loewenstein, G. 2012. "The Impact of Relative Standards on the Propensity to Disclose," Journal of Marketing Research (49:2), pp. 160-174.

Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making. *MIS Quarterly*, *42*(2), 465–488. https://doi.org/10.25300/misq/2018/14316.

Aharony, N. (2016). Relationships among attachment theory, social capital perspective, personality characteristics, and Facebook self-disclosure. *Aslib Journal of Information Management*, *68*(3), 362–386. https://doi.org/10.1108/ajim-01-2016-0001.

Ajzen, I. (2002, September). *Constructing a Theory of Planned Behavior Questionnaire*. https://www.researchgate.net/publication/235913732_Constructing_a_Theory_of_Planned_Behavior_Questionnaire.

Alexanderson, G. L., & Polya, G. (1979). Mathematics and Plausible Reasoning: Vol. I: Induction and Analogy in Mathematics. *The Two-Year College Mathematics Journal*, *10*(2), 119. https://doi.org/10.2307/302702.

Altman, I. and Taylor, D.A. (1973) Social Penetration: The Development of Interpersonal Relationships. Holt, Rinehart, & Winston, New York, 459.

Amazon.com*: Amazon Device Warranty*. (2022, May 18). Amazon. Retrieved July 18, 2022, from https://www.amazon.com/.

Angst, & Agarwal. (2009). Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. *MIS Quarterly*, *33*(2), 339. https://doi.org/10.2307/20650295.

Ansari, A., & Mela, C. F. (2003). E-Customization. *Journal of Marketing Research*, *40*(2), 131–145. https://doi.org/10.1509/jmkr.40.2.131.19224.

Arriaga, X. B., Kumashiro, M., Simpson, J. A., & Overall, N. C. (2017). Revising Working Models Across Time: Relationship Situations That Enhance Attachment Security. *Personality and Social Psychology Review*, *22*(1), 71–96. https://doi.org/10.1177/1088868317705257.

Ashfaq, M., Yun, J., & Yu, S. (2020). My Smart Speaker is Cool! Perceived Coolness, Perceived Values, and Users' Attitude toward Smart Speakers. *International Journal of Human–Computer Interaction*, *37*(6), 560–573. https://doi.org/10.1080/10447318.2020.1841404.

Awad, & 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. https://doi.org/10.2307/25148715.

Bagozzi, R. P. (1992). The Self-Regulation of Attitudes, Intentions, and Behavior. *Social Psychology Quarterly*, *55*(2), 178. https://doi.org/10.2307/2786945.

Barclay, D., Higgins, C. and Thompson, R. (1995), "The partial least squares (PLS) approach to causal modeling: personal computer adoption and use as an illustration",Technology Studies, Vol. 2 No. 2, pp. 285-309.

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

Bartneck, C., Lütge, C., Wagner, A., & Welsh, S. (2020). Privacy Issues of AI. *An Introduction to Ethics in Robotics and AI*, 61–70. https://doi.org/10.1007/978-3-030-51110-4_8.

BBC News. (2019, April 11). *Smart speaker recordings reviewed by humans*. Retrieved July 4, 2022, from https://www.bbc.com/news/technology-47893082.

Beldad, A. D. (2015). Sharing to be sociable, posting to be popular: factors influencing non-static personal information disclosure on Facebook among young Dutch users. *International Journal of Web Based Communities*, *11*(3/4), 357. https://doi.org/10.1504/ijwbc.2015.072132.

Bell, E. T., & Polya, G. (1945). How to Solve It. A New Aspect of Mathematical Method. *The American Mathematical Monthly*, *52*(10), 575. https://doi.org/10.2307/2306109

Bentley, F., Luvogt, C., Silverman, M., Wirasinghe, R., White, B., & Lottridge, D. (2018). Understanding the Long-Term Use of Smart Speaker Assistants. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *2*(3), 1–24. https://doi.org/10.1145/3264901.

Berscheid, Ellen, William Graziano, Thomas Monson, and Marshall Dermer (1976), "Outcome Dependency: Attention, Attribution, and Attraction," Journal of Personality and Social Psychology, 34 (5), 978-989.

Beuker, S. (2016). *Privacy Paradox: Factors Influencing Disclosure of Personal Information.* (93rd ed.) [E-book]. Master's Thesis. University of Twente.

Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, *37*(3), 466–480. https://doi.org/10.1016/j.ijresmar.2020.03.006.

Brandimarte, L., Acquisti, A., and Loewenstein, G. 2012. "Misplaced Confidences: Privacy and the Control Paradox," Social Psychological and Personality Science (4:3), pp. 340-347.

Bucy, E. P. (2017). Nonverbal Cues. *The International Encyclopedia of Media Effects*, 1–11. https://doi.org/10.1002/9781118783764.wbieme0199.

Burton-Jones, A., & Hubona, G. S. (2005). Individual differences and usage behavior. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *36*(2), 58–77. https://doi.org/10.1145/1066149.1066155.

Campbell, D. E., Parboteeah, D. V., & Dipascal, A. (2011). What Are Your Intentions: An Empirical Analysis of the Distinction between Behavioral Intentions and Behavioral Goals? *2011 44th Hawaii International Conference on System Sciences*. https://doi.org/10.1109/hicss.2011.491.

Cao, G., & Wang, P. (2022). Revealing or concealing privacy information disclosure in intelligent voice assistant usage- a configurational approach. *Industrial Management & Data Systems*, *122*(5), 1215–1245. https://doi.org/10.1108/imds-08-2021-0485

Catona, D., & Greene, K. (2015). Self-Disclosure. *The International Encyclopedia of Interpersonal Communication*, 1–5. https://doi.org/10.1002/9781118540190.wbeic162.

Cha, H. S., Wi, J. H., Park, C., & Kim, T. (2021). Sustainability Calculus in Adopting Smart Speakers—Personalized Services and Privacy Risks. *Sustainability*, *13*(2), 602. https://doi.org/10.3390/su13020602.

Chai, J., Weng, Z., & Liu, W. (2021). Behavioral Decision Making in Normative and Descriptive Views: A Critical Review of Literature. *Journal of Risk and Financial Management*, *14*(10), 490. https://doi.org/10.3390/jrfm14100490.

Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of Personality and Social Psychology*, *39*(5), 752–766. https://doi.org/10.1037/0022-3514.39.5.752.

Chakraborty, R., Vishik, C., & Rao, H. R. (2013). Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems*, *55*(4), 948–956. https://doi.org/10.1016/j.dss.2013.01.004.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management*, *6*(2–3), 181–202. https://doi.org/10.1007/s10799-005-5879-y.

Chitturi, R., Raghunathan, R., & Mahajan, V. (2008). Delight by Design: The Role of Hedonic Versus Utilitarian Benefits. Journal of Marketing, 72(3), 48–63. https://doi.org/10.1509/jmkg.72.3.48

Cialdini, R. B., & Goldstein, N. J. (2004). Social Influence: Compliance and Conformity. *Annual Review of Psychology*, *55*(1), 591–621. https://doi.org/10.1146/annurev.psych.55.090902.142015.

Cook, K. S., & Rice, E. (2006). Social Exchange Theory. *Handbook of Social Psychology*, 53–76. https://doi.org/10.1007/0-387-36921-x_3.

Coon, D., & Mitterer, J. O. (2008). Introduction to Psychology: Gateways to Mind and Behavior. *Cengage Learning*, 220.

Cozby, P. C. (1973). Self-disclosure: A literature review. *Psychological Bulletin*, *79*(2), 73–91. https://doi.org/10.1037/h0033950.

Dagger, T. S., Danaher, P. J., & Gibbs, B. J. (2008). How Often Versus How Long. *Journal of Service Research*, *11*(4), 371–388. https://doi.org/10.1177/1094670508331251.

Darlington, K. (2018, August 6). *The Emergence of the Age of AI*. OpenMind. Retrieved June 20, 2022, from https://www.bbvaopenmind.com/en/technology/artificial-intelligence/the-emergence-of-the-age-of-ai/.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319. https://doi.org/10.2307/249008.

De Bono, K. G., & Harnish, R. J. (1988). Source expertise, source attractiveness, and the processing of persuasive information: A functional approach. *Journal of Personality and Social Psychology*, *55*(4), 541–546. https://doi.org/10.1037/0022-3514.55.4.541.

Dewey, J. (2021). *How We Think: Original Classics and Annotated*. Independently published.

Dietrich, C. (2010, February 1). *Decision Making: Factors that Influence Decision Making, Heuristics Used, and Decision Outcomes*. Inquiries Journal. Retrieved June 20, 2022, from http://www.inquiriesjournal.com/articles/180/decision-making-factors-that-influence-decision-making-heuristics-used-and-decision-outcomes?id=180.

Dinev, T.; Hart, P (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. Inf. Syst. Res., 17, 61–80.

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Information Systems Research*, *26*(4), 639–655. https://doi.org/10.1287/isre.2015.0600.

DiPiazza, S. A., & Eccles, R. G. (2002). Building public trust: The future of corporate reporting. New York: Wiley.

Egelman, S., Felt, A. P., and Wagner, D. (2013). "Choice Architecture and Smartphone Privacy: There's a Price for That," in The Economics of Information Security and Privacy, R. Böhme (ed.), Berlin: Springer, pp. 211-236.

E Petty, R., & t Cacioppo, J. (1986). The Elaboration Likelihood Model of Persuasion. *Advances in Experimental Social Psychology*, *19*(1), 124–205.

Fan, A., Wu, Q., Yan, X., Lu, X., Ma, Y., & Xiao, X. (2021). Research on Influencing Factors of Personal Information Disclosure Intention of social media in China. *Data and Information Management*, *5*(1), 195–207. https://doi.org/10.2478/dim-2020-0038.

Fehr, E., & Gächter, S. (2000). Fairness and Retaliation: The Economics of Reciprocity. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.260736.

Ferrell, O. C. (2016). Broadening marketing's contribution to data privacy. *Journal of the Academy of Marketing Science*, *45*(2), 160–163. https://doi.org/10.1007/s11747-016-0502-9.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50. https://doi.org/10.2307/3151312.

Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics*, *22*(3), 167–176. https://doi.org/10.1016/j.iedeen.2016.04.002.

Frost-Arnold, K. (2012). The cognitive attitude of rational trust. *Synthese*, *191*(9), 1957–1974. https://doi.org/10.1007/s11229-012-0151-6.

Fruchter, N., & Liccardi, I. (2018). Consumer Attitudes Towards Privacy and Security in Home Assistants. *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3170427.3188448.

Gable, S. L., & Reis, H. T. (1999). Now and then, them and us, this and that: Studying relationships across time, partner, context, and person. *Personal Relationships*, *6*(4), 415–432. https://doi.org/10.1111/j.1475-6811.1999.tb00201.x.

Garg, R., & Sengupta, S. (2020). He Is Just Like Me. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *4*(1), 1–24. https://doi.org/10.1145/3381002.

Garrotes, P. S. M. S. (2021, October). *EXPLORING THE ENGAGEMENT PROCESS BETWEEN HUMANS AND INTELLIGENT VIRTUAL ASSISTANTS*. https://repositorio.iscte-iul.pt/bitstream/10071/23920/1/master_patricia_silva_garrotes.pdf.

Gauch, S., Speretta, M., Chandramouli, A., & Micarelli, A. (2007). User Profiles for Personalized Information Access. *The Adaptive Web*, 54–89. https://doi.org/10.1007/978-3-540-72079-9_2.

Gerbing, D., & Anderson, J. (1988). An updated paradigm for scale development incorporating unidimensionality and its assessment. Journal of Marketing Research, 25(2), 186–192.

Gigerenzer, G., & Gaissmaier, W. (2011). Heuristic Decision Making. *Annual Review of Psychology*, *62*(1), 451–482. https://doi.org/10.1146/annurev-psych-120709-145346.

Gigerenzer, G., Hoffrage, U., & Kleinbölting, H. (1991). Probabilistic mental models: A Brunswikian theory of confidence. *Psychological Review*, *98*(4), 506–528. https://doi.org/10.1037/0033-295x.98.4.506.

Gomes, A. R., Gonçalves, A. M., Maddux, J. E., & Carneiro, L. (2017). The intention-behaviour gap: An empirical examination of an integrative perspective to explain exercise behaviour. *International Journal of Sport and Exercise Psychology*, *16*(6), 607–621. https://doi.org/10.1080/1612197x.2017.1321030.

Grayson, K., & Ambler, T. (1999). The Dark Side of Long-Term Relationships in Marketing Services. *Journal of Marketing Research*, *36*(1), 132. https://doi.org/10.2307/3151921

Greene, K., Derlega, V. J., & Mathews, A. (2006). Self-Disclosure in Personal Relationships. *The Cambridge Handbook of Personal Relationships*, 409–428. https://doi.org/10.1017/cbo9780511606632.023.

Haack, W., Severance, M., Wallace, M., & Wohlwend, J. (2017). Security Analysis of the Amazon Echo. *Allen Institute for Artificial Intelligence*, 208–220.

Hair, Joseph F., Ronald L. Tatham, Rolph E. Anderson, and William Black. (1998). Multivariate Analysis. 5th edition. Upper Saddle River, NJ: Prentice Hall

Hair, J. F., Howard, M. C., & Nitzl, C. (2020). Assessing measurement model quality in PLS-SEM using confirmatory composite analysis. *Journal of Business Research*, *109*, 101–110. https://doi.org/10.1016/j.jbusres.2019.11.069.

Han, S., & Yang, H. (2018). Understanding adoption of intelligent personal assistants. *Industrial Management & Data Systems*, *118*(3), 618–636. https://doi.org/10.1108/imds-05-2017-0214.

Hanczakowski, M., Pasek, T., Zawadzka, K., & Mazzoni, G. (2013). Cue familiarity and 'don't know' responding in episodic memory tasks. *Journal of Memory and Language*, *69*(3), 368–383. https://doi.org/10.1016/j.jml.2013.04.005.

Hassan, L. M., Shiu, E., & Shaw, D. (2014). Who Says There is an Intention–Behaviour Gap? Assessing the Empirical Evidence of an Intention–Behaviour Gap in Ethical

Consumption. *Journal of Business Ethics*, *136*(2), 219–236. https://doi.org/10.1007/s10551-014-2440-0.

Hauswald, J., Laurenzano, M. A., Zhang, Y., Li, C., Rovinski, A., Khurana, A., Dreslinski, R. G., Mudge, T., Petrucci, V., Tang, L., & Mars, J. (2015). Sirius. *ACM SIGPLAN Notices*, *50*(4), 223–238. https://doi.org/10.1145/2775054.2694347.

Hertwig, R., & Herzog, S. M. (2009). Fast and Frugal Heuristics: Tools of Social Rationality. *Social Cognition*, *27*(5), 661–698. https://doi.org/10.1521/soco.2009.27.5.661.

Hsee, C. K. (1996). The Evaluability Hypothesis: An Explanation for Preference Reversals between Joint and Separate Evaluations of Alternatives. *Organizational Behavior and Human Decision Processes*, *67*(3), 247–257. https://doi.org/10.1006/obhd.1996.0077.

Hsee, C. K., Loewenstein, G. F., Blount, S., & Bazerman, M. H. (1999). Preference reversals between joint and separate evaluations of options: A review and theoretical analysis. *Psychological Bulletin*, *125*(5), 576–590.https://doi.org/10.1037/0033-2909.125.5.576

Hui, Teo, & Lee. (2007). The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly*, *31*(1), 19. https://doi.org/10.2307/25148779.

IBM. *(2022). SPSS statistical software:* Release 2015. IBM.

IBM. *SPSS Amos (2022).* Version 26. Release 2019. IBM. https://www.ibm.com/products/structural-equation-modeling-sem.

Ioannou, A., Tussyadiah, I., Miller, G., Li, S., & Weick, M. (2021). Privacy nudges for disclosure of personal information: A systematic literature review and meta-analysis. *PLOS ONE*, *16*(8), e0256822. https://doi.org/10.1371/journal.pone.0256822.

J., E., & James, M. (2012, September 21). *Social Penetration Theory*. Communication Studies.https://www.communicationstudies.com/communication-theories/social-penetration-theory.

John, L., Acquisti, A., and Loewenstein, G. 2011. "Strangers on a Plane: Context Dependent Willingness to Divulge Personal Information," Journal of Consumer Research (37:5), pp. 858-873.

Joinson, A., Reips, U. D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, Trust, and Self-Disclosure Online. *Human-Computer Interaction*, *25*(1), 1–24. https://doi.org/10.1080/07370020903586662.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263. https://doi.org/10.2307/1914185.

Kammoun, A., Slama, R., Tabia, H., Ouni, T., & Abid, M. (2022). Generative Adversarial Networks for face generation: A survey. *ACM Computing Surveys*. https://doi.org/10.1145/1122445.1122456.

Kang, M. J., Rangel, A., Camus, M., & Camerer, C. F. (2011). Hypothetical and Real Choice Differentially Activate Common Valuation Areas. *Journal of Neuroscience*, *31*(2), 461–468. https://doi.org/10.1523/jneurosci.1583-10.2011.

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

Kehr, F., Wentzel, D., & Mayer, P. (2013). *Rethinking the Privacy Calculus: On the Role of Dispositional Factors and Affect*. AIS Association for Information Systems. https://www.alexandria.unisg.ch/publications/224696.

Keith, M. J., Babb, J. S., & Lowry, P. B. (2014). A Longitudinal Study of Information Privacy on Mobile Devices. *2014 47th Hawaii International Conference on System Sciences*. https://doi.org/10.1109/hicss.2014.391.

Kemper, T. D. (1973). The Fundamental Dimensions of Social Relationship: a Theoretical Statement. *Acta Sociologica*, *16*(1), 41–60. https://doi.org/10.1177/000169937301600104.

Khan, A. N., Pitafi, A. H., & Kanwal, S. (2020). Effects of perceived ease of use on SNSs-addiction through psychological dependence, habit: the moderating role of perceived usefulness. *International Journal of Business Information Systems*, *33*(3), 383. https://doi.org/10.1504/ijbis.2020.10027455.

Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273–281. https://doi.org/10.1016/j.chb.2018.11.022.

Kinsella, B. (2019, June 21). *Voice Assistant Demographic Data - Young Consumers More Likely to Own Smart Speakers While Over 60 Bias Toward Alexa and Siri*. Voicebot.Ai. Retrieved July 6, 2022, from https://voicebot.ai/2019/06/21/voice-assistant-demographic-data-young-consumers-more-likely-to-own-smart-speakers-while-over-60-bias-toward-alexa-and-siri/.

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

Krist, C., Schwarz, C. V., & Reiser, B. J. (2018). Identifying Essential Epistemic Heuristics for Guiding Mechanistic Reasoning in Science Learning. *Journal of the Learning Sciences*, *28*(2), 160–205. https://doi.org/10.1080/10508406.2018.1510404.

Lahlou, S.; Langheinrich, M.; Röcker, C. Privacy and trust issues with invisible computers. Commun. ACM 2005, 48, 59–60.

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, Are You Listening? *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1–31. https://doi.org/10.1145/3274371.

Lewicki, R. J., McAllister, D. J., & Bies, R. J. (1998). Trust and Distrust: New Relationships and Realities. *The Academy of Management Review*, *23*(3), 438. https://doi.org/10.2307/259288.

Li, C. R., Zhang, E., & Han, J. T. (2021). Adoption of online follow-up service by patients: An empirical study based on the elaboration likelihood model. *Computers in Human Behavior*, *114*, 106581. https://doi.org/10.1016/j.chb.2020.106581.

Li, Z., & Rau, P. L. P. (2019). Effects of Self-Disclosure on Attributions in Human–IoT Conversational Agent Interaction. *Interacting with Computers*, *31*(1), 13–26. https://doi.org/10.1093/iwc/iwz002.

Limited, T. (2018, April 8). *Relationships: Social Exchange Theory*. Tutor2u. https://www.tutor2u.net/psychology/reference/relationships-social-exchange-theory#:%7E:text=According%20to%20Social%20Exchange%20Theory,more%20profitable%20than%20the%20alternatives.

Lin, Y., & Boh, W. F. (2021). Informational cues or content? Examining project funding decisions by crowdfunders. *Information & Management*, *58*(7), 103499. https://doi.org/10.1016/j.im.2021.103499.

Lockey, S., Gillespie, N., Holm, D., & Someh, I. A. (2021). A Review of Trust in Artificial Intelligence: Challenges, Vulnerabilities and Future Directions. *Proceedings of the Annual Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2021.664.

Marmion, V., Bishop, F., Millard, D. E., & Stevenage, S. V. (2017). The Cognitive Heuristics Behind Disclosure Decisions. *Lecture Notes in Computer Science*, 591–607. https://doi.org/10.1007/978-3-319-67217-5_35.

Marsh, S., Dibben, M.R. (2005). Trust, Untrust, Distrust and Mistrust – An Exploration of the Dark(er) Side. In P. Herrmann, Issarny, V., Shiu, S. (Eds.), Trust Management, Third International Conference Proceedings, iTrust 2005 (pp. 17-33).

Martin, K. D., & Murphy, P. E. (2016). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155. https://doi.org/10.1007/s11747-016-0495-4.

Meinert, J., & Krämer, N. C. (2022). How the expertise heuristic accelerates decision-making and credibility judgments in social media by means of effort reduction. *PLOS ONE*, *17*(3), e0264428. https://doi.org/10.1371/journal.pone.0264428.

Metzger, M. J., Flanagin, A. J., & Medders, R. B. (2010). Social and Heuristic Approaches to Credibility Evaluation Online. *Journal of Communication*, *60*(3), 413–439. https://doi.org/10.1111/j.1460-2466.2010.01488.x.

Metzger, M. J., & Flanagin, A. J. (2013). Credibility and trust of information in online environments: The use of cognitive heuristics. *Journal of Pragmatics*, *59*, 210–220. https://doi.org/10.1016/j.pragma.2013.07.012.

Metzger MJ, Flanagin AJ (2015). Psychological approaches to credibility assessment online. In: Sundar SS, editor. The Handbook of the Psychology of Communication Technology. Chichester, UK: John Wiley & Sons, Inc.;. p. 445–466.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15–29. https://doi.org/10.1002/dir.20009.

Mondak, J. J. (1993). Public opinion and heuristic processing of source cues. *Political Behavior*, *15*(2), 167–192. https://doi.org/10.1007/bf00993852.

Moorman, C., Zaltman, G., & Deshpande, R. (1992). Relationships between Providers and Users of Market Research: The Dynamics of Trust within and between Organizations. *Journal of Marketing Research*, *29*(3), 314. https://doi.org/10.2307/3172742.

Mukherjee, S. (2012, December 19). *Anchoring - An NLP Master Tool*. Https://Papers.Ssrn.Com/Sol3/Papers.Cfm?Abstract_id=2191435. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2191435.

Nass, C., & Moon, Y. (2000). Machines and Mindlessness: Social Responses to Computers. *Journal of Social Issues*, *56*(1), 81–103. https://doi.org/10.1111/0022-4537.00153.

Nicholson, Carolyn Y., Larry D. Compeau, and Rajesh Sethi (2001), "The Role of Interpersonal Liking in Building Trust in Long-Term Channel Relationships," Journal of the Academy of Marketing Science, 29 (1), 3-13.

Niether, D., & Wiegand, S. (2017). Heuristic Approach to Understanding the Accumulation Process in Hydrothermal Pores. *Entropy*, *19*(1), 33. https://doi.org/10.3390/e19010033.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x.

Nunnelly, J.C. (1978), Psychometric Theory, McGraw-Hill, New York, NY.

Pal, D., Arpnikanondt, C., & Razzaque, M. A. (2020). Personal Information Disclosure via Voice Assistants: The Personalization–Privacy Paradox. *SN Computer Science*, *1*(5). https://doi.org/10.1007/s42979-020-00287-9.

Palmatier, R. W., Houston, M. B., Dant, R. P., & Grewal, D. (2013). Relationship Velocity: Toward a Theory of Relationship Dynamics. *Journal of Marketing*, *77*(1), 13–30. https://doi.org/10.1509/jm.11.0219.

Pan, W., Feng, B., Wingate, V. S., & Li, S. (2020). What to Say When Seeking Support Online: A Comparison Among Different Levels of Self-Disclosure. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.00978.

Papies, E. K. (2017). Situating interventions to bridge the intention-behaviour gap: A framework for recruiting nonconscious processes for behaviour change. *Social and Personality Psychology Compass*, *11*(7), e12323. https://doi.org/10.1111/spc3.12323.

Paramarta, V., Jihad, M., Dharma, A., Hapsari, I. C., Sandhyaduhita, P. I., & Hidayanto, A. N. (2018). Impact of User Awareness, Trust, and Privacy Concerns on Sharing Personal Information on social media: Facebook, Twitter, and Instagram. *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*. https://doi.org/10.1109/icacsis.2018.8618220.

Park, K., Kwak, C., Lee, J., & Ahn, J. H. (2018). The effect of platform characteristics on the adoption of smart speakers: Empirical evidence in South Korea. *Telematics and Informatics*, *35*(8), 2118–2132. https://doi.org/10.1016/j.tele.2018.07.013.

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

Peacock, C. E., & Ekstrom, A. D. (2018). Verbal cues flexibly transform spatial representations in human memory. *Memory*, *27*(4), 465–479. https://doi.org/10.1080/09658211.2018.1520890.

Pearce, W. B., & Sharp, S. M. (1973). Self-Disclosing Communication. *Journal of Communication*, *23*(4), 409–425. https://doi.org/10.1111/j.1460-2466.1973.tb00958.x

Pee, L. G., & Lee, J. (2016). Trust in User-Generated Information on Social Media during Crises : An Elaboration Likelihood Perspective. *Asia Pacific Journal of Information Systems*, *26*(1), 1–22. https://doi.org/10.14329/apjis.2016.26.1.1.

Petty, R. E., Cacioppo, J. T., & Schumann, D. (1983). Central and Peripheral Routes to Advertising Effectiveness: The Moderating Role of Involvement. *Journal of Consumer Research*, *10*(2), 135. https://doi.org/10.1086/208954.

Picchi, A. (2019, April 12). *Amazon Alexa: Workers are paid to listen to consumer conversations*. CBS News. Retrieved July 4, 2022, from https://www.cbsnews.com/news/amazon-workers-are-listening-to-what-you-tell-alexa/.

Plangger, K., & Montecchi, M. (2020). Thinking beyond Privacy Calculus: Investigating Reactions to Customer Surveillance. *Journal of Interactive Marketing*, *50*(1), 32–44. https://doi.org/10.1016/j.intmar.2019.10.004.

Qualtrics XM // The Leading Experience Management Software. (2022, July 14). Qualtrics. https://www.qualtrics.com/.

Riemer, K.; Totz, C. (2010) The many faces of personalization? An integrative economic overview of mass-customization and personalization. In Proceedings of the World Conference on Mass Customization, Personalization, and Co-Creation, Hong Kong, China,.

Risius, M., Baumann, A., & Krasnova, H. (2020, June). Developing a New Paradigm: Introducing the Intention-Behaviour Gap to the Privacy Paradox Phenomenon. In Frantz Rowe, Redouane El Amrani, Moez Limayem, Sue Newell, Nancy Pouloudi, Eric van Heck, Ali El Quammah, (Ed.), *28th European Conference on Information Systems - Liberty, Equality, and Fraternity in a Digitizing World*. ECIS 2020.

Schirrmeister, E., Göhring, A., & Warnke, P. (2020). Psychological biases and heuristics in the context of foresight and scenario processes. *FUTURES & FORESIGHT SCIENCE*, *2*(2). https://doi.org/10.1002/ffo2.31.

Scheen, M. (2014). The Effects of Trust and Distrust on Privacy Risk Perception. *Chair Group: Marketing and Consumer Behaviour. Master Thesis*, 1–34.

Seymour, W., & van Kleek, M. (2021). Exploring Interactions Between Trust, Anthropomorphism, and Relationship Development in Voice Assistants. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW2), 1–16. https://doi.org/10.1145/3479515.

Schwikert, S. R., & Curran, T. (2014). Familiarity and recollection in heuristic decision making. *Journal of Experimental Psychology: General*, *143*(6), 2341–2365. https://doi.org/10.1037/xge0000024.

Shah, A. K., & Oppenheimer, D. M. (2008). Heuristics made easy: An effort-reduction framework. *Psychological Bulletin*, *134*(2), 207–222. https://doi.org/10.1037/0033-2909.134.2.207.

Sharif, A., Soroya, S. H., Ahmad, S., & Mahmood, K. (2021). Antecedents of Self-Disclosure on Social Networking Sites (SNSs): A Study of Facebook Users. *Sustainability*, *13*(3), 1220. https://doi.org/10.3390/su13031220.

Sheeran, P. (2005). Intention-Behavior Relations: A Conceptual and Empirical Review. *European Review of Social Psychology*, 1–36. https://doi.org/10.1002/0470013478.ch1.

Shen, A., & Dwayne Ball, A. (2009). Is personalization of services always a good thing? Exploring the role of technology-mediated personalization (TMP) in service relationships. *Journal of Services Marketing*, *23*(2), 79–91. https://doi.org/10.1108/08876040910946341.

Shih, D. H., Hsu, S. F., Yen, D. C., & Lin, C. C. (2012). Exploring the Individual's Behavior on Self-Disclosure Online. *International Journal of Human-Computer Interaction*, *28*(10), 627–645. https://doi.org/10.1080/10447318.2011.654198.

Shrestha, N. (2020). Detecting Multicollinearity in Regression Analysis. *American Journal of Applied Mathematics and Statistics*, *8*(2), 39–42. https://doi.org/10.12691/ajams-8-2-1.

Smith, Dinev, & Xu. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989. https://doi.org/10.2307/41409970.

Stankutė-Søsted, R. (2019). The Susceptibility of Lithuanian Youth to Information Attacks: the Elaboration Likelihood Model and Presumable Attack Topics. *Lithuanian Annual Strategic Review*, *17*(1), 335–359. https://doi.org/10.2478/lasr-2019-0014.

Statista. (2022, March 28). *Main smart speaker use cases in the U.S. 2020*. Retrieved July 1, 2022, from https://www.statista.com/statistics/994696/united-states-smart-speaker-use-case-frequency/.

Sternberg, R. J. (1986). A triangular theory of love. *Psychological Review*, *93*(2), 119–135. https://doi.org/10.1037/0033-295x.93.2.119.

Stewart, D. D., Stewart, C. B., Tyson, C., Vinci, G., & Fioti, T. (2004). Serial Position Effects and the Picture-Superiority Effect in the Group Recall of Unshared Information. *Group Dynamics: Theory, Research, and Practice*, *8*(3), 166–181. https://doi.org/10.1037/1089-2699.8.3.166.

Steyerberg, E. W. (2016). FRANK E. HARRELL, Jr., Regression Modeling Strategies: With Applications, to Linear Models, Logistic and Ordinal Regression, and Survival Analysis, 2nd ed. Heidelberg: Springer. *Biometrics*, *72*(3), 1006–1007. https://doi.org/10.1111/biom.12569.

Sun, C. C. (2021). Analyzing Determinants for Adoption of Intelligent Personal Assistant: An Empirical Study. *Applied Sciences*, *11*(22), 10618. https://doi.org/10.3390/app112210618.

Sun, Q., Willemsen, M. C., & Knijnenburg, B. P. (2020). Unpacking the intention-behavior gap in privacy decision making for the internet of things (IoT) using aspect listing. *Computers & Security*, *97*, 101924. https://doi.org/10.1016/j.cose.2020.101924

Sun, Y., Fang, S., & Hwang, Y. (2019). Investigating Privacy and Information Disclosure Behavior in Social Electronic Commerce. *Sustainability*, *11*(12), 3311. https://doi.org/10.3390/su11123311.

Swann, William B. and Michael J. Gill (1997), "Confidence and Accuracy in Person Perception: Do We Know What We Think about Our Relationship Partners?" Journal of Personality and Social Psychology, 73 (4), 747-757.

Tai, M. T. (2020). The impact of artificial intelligence on human society and bioethics. *Tzu Chi Medical Journal*, *32*(4), 339. https://doi.org/10.4103/tcmj.tcmj_71_20.

Taylor, D. A. (1968). The Development of Interpersonal Relationships: Social Penetration Processes. *The Journal of Social Psychology*, *75*(1), 79–90. https://doi.org/10.1080/00224545.1968.9712476.

Terzopoulos, G., & Satratzemi, M. (2020). Voice Assistants and Smart Speakers in Everyday Life and in Education. *Informatics in Education*, 473–490. https://doi.org/10.15388/infedu.2020.21.

Tolstedt, B. E., & Stokes, J. P. (1984). Self-disclosure, intimacy, and the depenetration process. *Journal of Personality and Social Psychology*, *46*(1), 84–90. https://doi.org/10.1037/0022-3514.46.1.84

Sphweb website. *The Theory of Planned Behavior*. (2019, September). Consulted in July 2022. https://sphweb.bumc.bu.edu/otlt/mph-modules/sb/behavioralchangetheories/BehavioralChangeTheories3.html.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, *22*(2), 254–268. https://doi.org/10.1287/isre.1090.0260.

Tullis, J. G. (2018b). Predicting others' knowledge: Knowledge estimation as cue utilization. *Memory & Cognition*, *46*(8), 1360–1375. https://doi.org/10.3758/s13421-018-0842-4.

Turilli, M., & Floridi, L. (2009). The ethics of information transparency. *Ethics and Information Technology*, *11*(2), 105–112. https://doi.org/10.1007/s10676-009-9187-9.

Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science*, *185*(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124.

Uelsen, A. V. (2021). Usefulness vs. Uncanniness: Exploring the perceived usefulness of virtual assistants in the customer journey. *University of Twente*, 1–12.

Understanding Social Exchange Theory in Psychology. (2022, February 25). Very well Mind. Retrieved June 20, 2021, from https://www.verywellmind.com/what-is-social-exchange-theory-2795882.

Uysal, E., Alavi, S., & Bezençon, V. (2022). Trojan horse or useful helper? A relationship perspective on artificial intelligence assistants with humanlike features. *Journal of the Academy of Marketing Science*. https://doi.org/10.1007/s11747-022-00856-9.

Vanneste, B., Puranam, P., & Kretschmer, T. (2012). Trust Over Time in Exchange Relationships: Theory and Meta-Analysis. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1523209.

Van Stralen, D., & Mercer, T. (2021). High Reliability Organizing (HRO) is the Extension of Neonatology during Pandemic COVID-19. *Neonatology Today*, *16*(5), 97–109. https://doi.org/10.51362/neonatology.today/2021516597109.

Van Stralen, D., & Mercer, T. (2021). Inductive Processes, Heuristics, and Biases Modulated by High-Reliability Organizing (HRO) for COVID-19 and Disasters. *Neonatology Today*, *16*(9), 104–112. https://doi.org/10.51362/neonatology.today/20219169104112

Venkatesh, V. (2000). Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4062395.

Wang, C., & Wu, L. (2012). Customer loyalty and the role of relationship length. *Managing Service Quality: An International Journal*, *22*(1), 58–74. https://doi.org/10.1108/09604521211198119.

Wang, L., Hu, H. H., Yan, J., & Mei, M. Q. (2019). Privacy calculus or heuristic cues? The dual process of privacy decision making on Chinese social media. *Journal of Enterprise Information Management*, *33*(2), 353–380. https://doi.org/10.1108/jeim-05-2019-0121.

Webb, T. L., & Sheeran, P. (2006). Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence. *Psychological Bulletin*, *132*(2), 249–268. https://doi.org/10.1037/0033-2909.132.2.249.

Wiktor Krawczyk, M. ł., & Rachubik, J. (2019). Judgement and Decision making. *The Representativeness Heuristic and the Choice of Lottery Tickets: A Field Experiment*, *14*(1), 51–57.

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, *28*(3), 889–897. https://doi.org/10.1016/j.chb.2011.12.008.

Wu, Z.; Li, G.; Liu, Q.; Xu, G.; Chen, E. (2018). Covering the Sensitive Subjects to Protect Personal Privacy in Personalized Recommendation. IEEE Trans. Serv. Comput.11, 49–506.

Xiao, M., & Taylor, W. B. (2020, April). *AI-Mediated Exchange Theory*. https://doi.org/10.48550/arXiv.2003.02093.

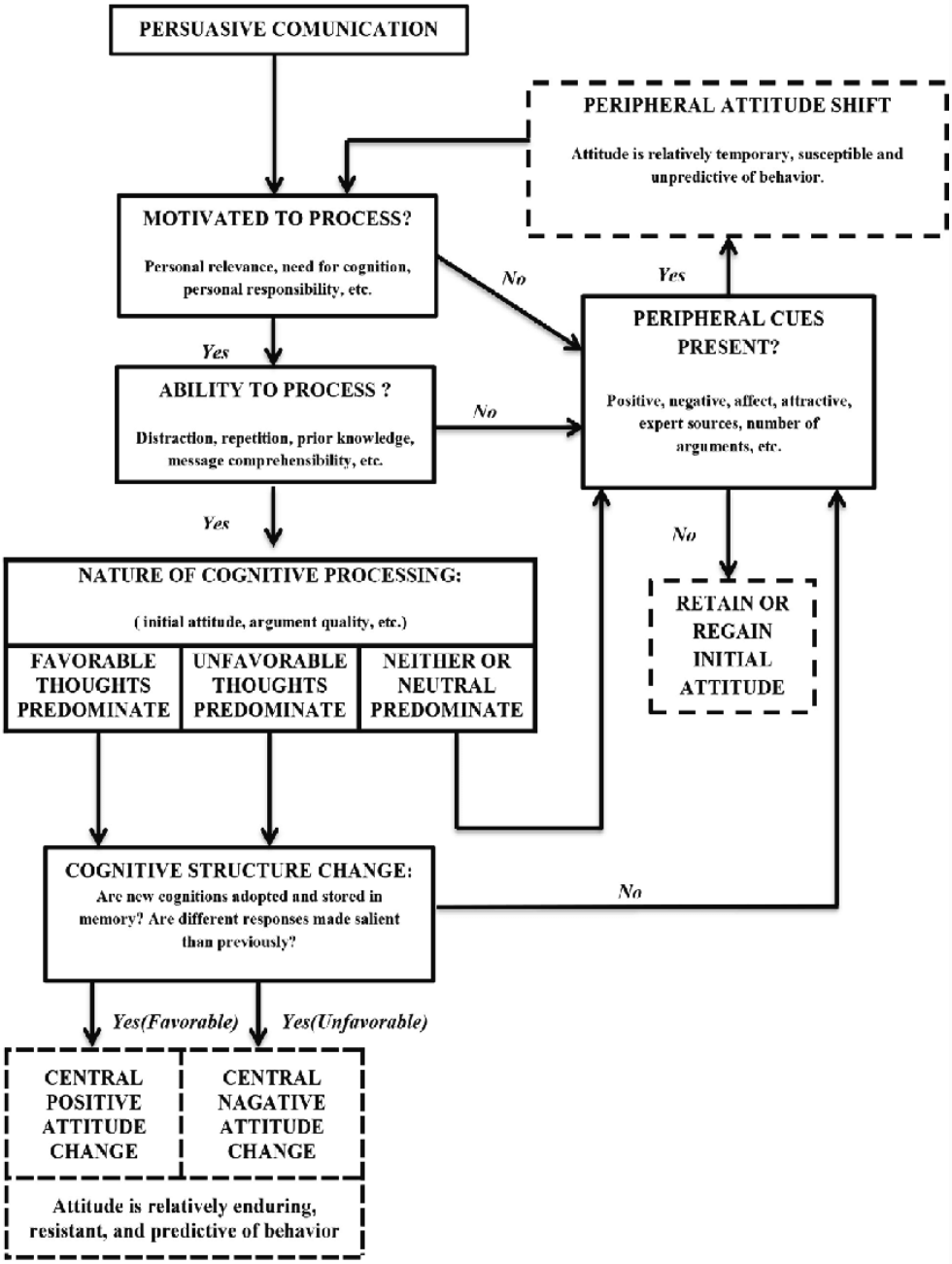
Yaakobi, E., & Goldenberg, J. (2014). Social relationships and information dissemination in virtual social network systems: An attachment theory perspective. *Computers in Human Behavior*, *38*, 127–135. https://doi.org/10.1016/j.chb.2014.05.025.

Yeung, C. W. M., & Soman, D. (2007). The Duration Heuristic. *Journal of Consumer Research*, *34*(3), 315–326. https://doi.org/10.1086/519500.

Yu, T. (2014). Gender Differences on Self-disclosure in Face-to-Face Versus E-mail Communication. *Proceedings of the International Conference on Education, Language, Art and Intercultural Communication*. https://doi.org/10.2991/icelaic-14.2014.184.

9. APPENDICES

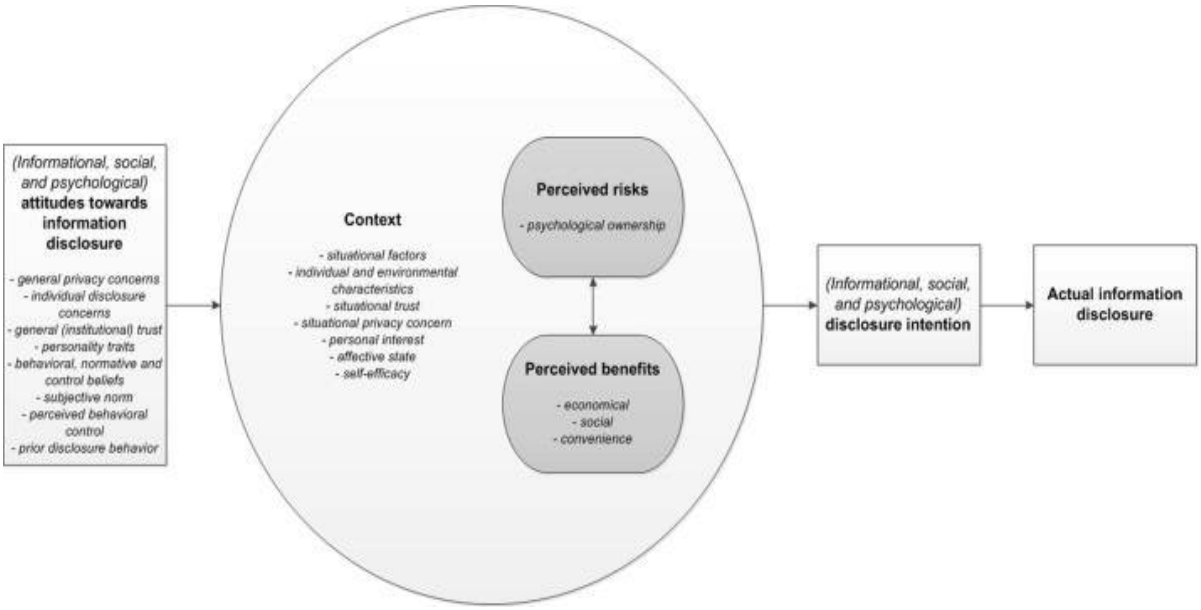
APPENDIX 1: SCHEMA OF ELABORATION LIKEHOOD MODEL



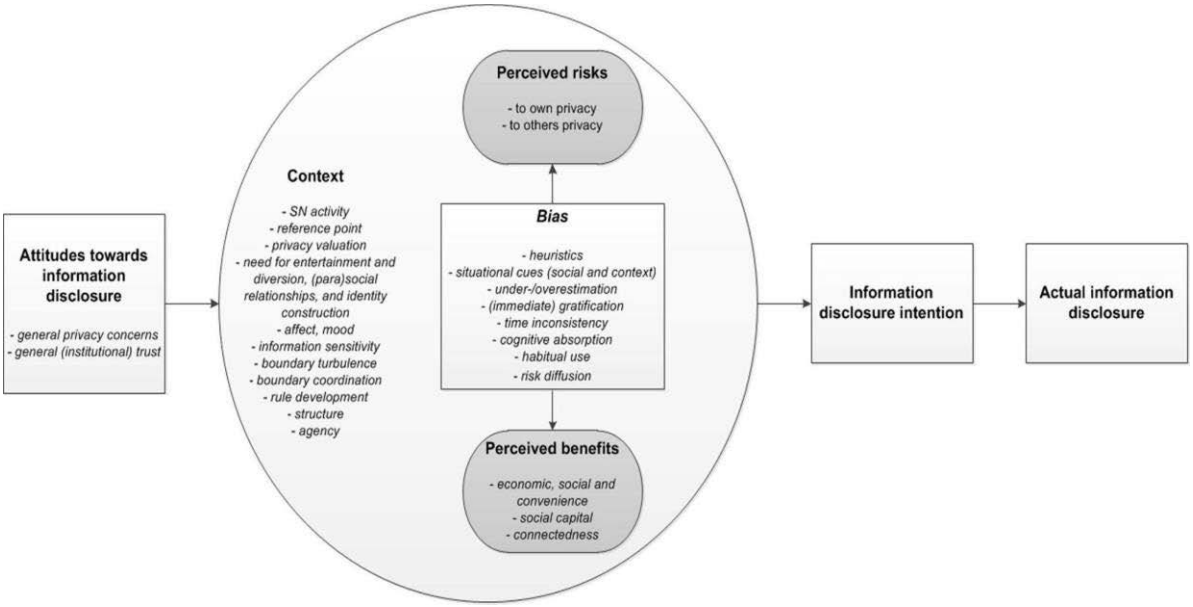
Source: Retrieved from Stankutė-Søsted, R. (2019). The Susceptibility of Lithuanian Youth to Information Attacks: The Elaboration Likelihood Model and Presumable Attack Topics. *Lithuanian Annual Strategic Review*, *17*(1), 335–359. https://doi.org/10.2478/lasr-2019-0014

APPENDIX 2: PRIVACY PARADOX MODEL (THE THREE DIFFERENT DECISION-MAKING PROCESSES)

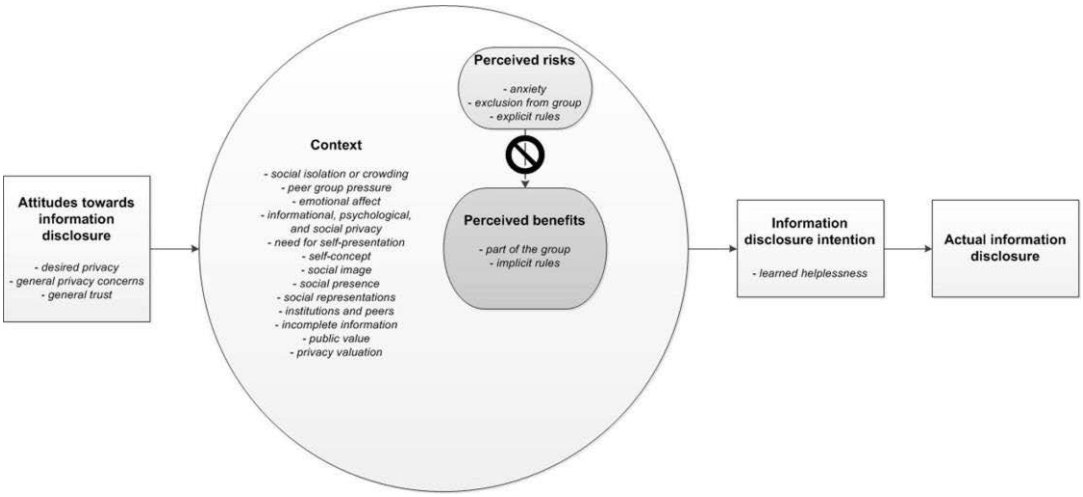
RATIONAL THINKING



SEMI-RATIONAL THINKING



NON-RATIONAL THINKING



Source: Retrieved from Barth, S., & de Jong, M. D. (2017a). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058.

APPENDIX 3: SUMMARIES OF PREVIOUS INTENTION-BEHAVIOR GAP RESEARCH

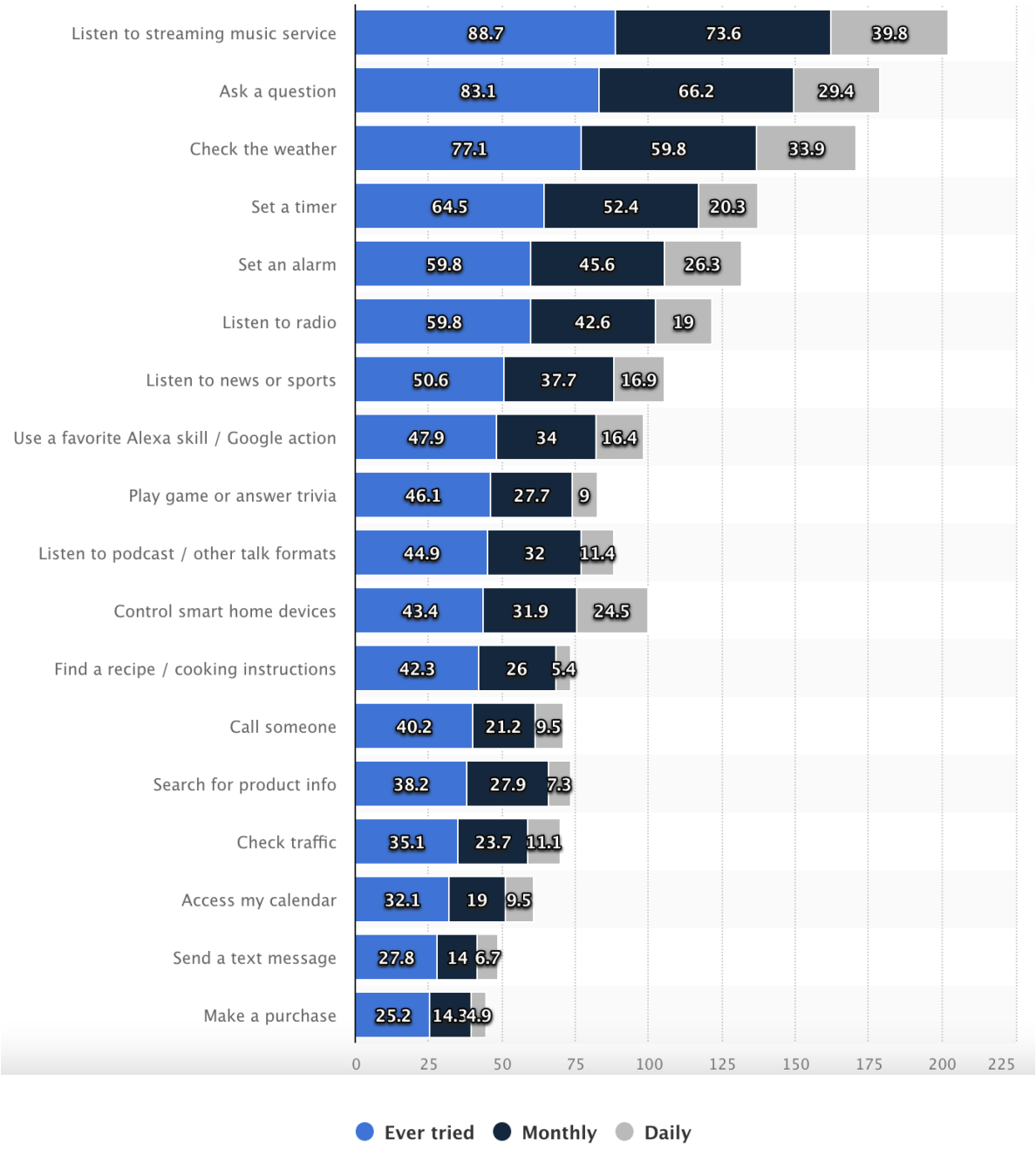
Author	Category	Methods	Main findings
Adjerid, I., Peer, E., & Acquisti, A. (2018).	Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making.	Experimental method	The objective and relative changes in privacy protection can affect hypothetical and actual self-disclosure behavior.
Norberg, P. A., Horne, D. R., & Horne, D. A. (2007).	The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors.	Empirical research (survey)	Researchers found that the level of actual disclosure exceeded intentions to disclose. Besides, two antecedents, risk, and trust, are measured to determine this gap. Risk admits influencing intention compared to actual disclosure and trust do not have any effect on actual behavioral disclosure.
Risius, M., Baumann, A., & Krasnova, H. (2020, June).	Introducing the Intention-Behaviour Gap to the Privacy Paradox Phenomenon	Experimental method	Researchers admit that intention is predictor to self-disclosure but within a certain gap. They introduced 3 antecedents to fill this gap. It confirmed to have a significant effect on translating intention into action: commitment, volitional strength and privacy concerns.
Sun, Q., Willemsen, M. C., & Knijnenburg, B. P. (2020).	The intention-behavior gap in privacy decision making for the internet of things (IoT) using aspect listing.	Empirical research (survey)	The findings observed a reversed intention-behavior gap in IoT. Individuals disclosed less (rather than more) information compared to their intentions based on decision type priority (i.e., risk outweigh benefit). The neutral decision type nullifies this reverse gap.

APPENDIX 4: SURVEY AND ITEMS LISTING

Variables	Items & Sources	Measurements
Privacy Concern	Please indicate how much you agree with the following statements. ● It is very important to me that I am knowledgeable about how my personal information will be used. ● I am worried Smart Speaker/Smart Personal Assistant will share my personal information with other firms. ● It bothers me to give my personal information to Smart Speaker/Smart Personal Assistant.	7 points Likert scales (1=Strongly disagree… 7=Strongly agree)
Perceived benefit	Please indicate how much you agree with the following statements. Disclosing information to Smart Speaker/Smart Personal Assistant ● …can provide me with personalized services. ● …ensures productivity to my mundane tasks. ● …can provide me with entertainment.	7 points Likert scales (1=Strongly disagree… 7=Strongly agree)
Information to Privacy protection	Please indicate how much you agree with the following statements. I am informed ● …how my personal information will be used by Smart Speaker/smart virtual assistant. ● …how my personal information will be stored by Smart Speaker/smart virtual assistant. ● …how my personal information will be protected by Smart Speaker/smart virtual assistant.	7 points Likert scales (1=Strongly disagree… 7=Strongly agree)
Relationship length	How long have you used a Smart Speaker/Smart Personal Assistant? ● … I do not use Smart Speaker/Smart Personal Assistant ● …Less than 1 year ● …1-2 years ● … 2-3 years ● …3-4 years ● …More than 4	Single choice question years Developed from the Preference for Technology survey-Classroom Edition

Variables	Items & Sources	Measurements
Actual disclosure	Please indicate how often you have done these actions in the following statements. How often… AIA's users ● …have you disclosed your credit card information for Smart Virtual Assistant's purchase feature? ● …have you updated your address location to be used by Smart Virtual Assistant? ● …have you updated your phone number to be used by Smart Virtual Assistant? ● …did you allow your personal photos to be used by Smart Virtual Assistant? ● …did you delete your information search history stored by your Smart Virtual assistant? AIA's nonusers ● …have you disclosed your credit card information for online purchase? ● …have you updated your address location to be displayed online? ● …have you updated your phone number to be displayed online? ● …did you allow your personal photos to be displayed online? ● …did you delete your online search history?	5 points Likert scales (1=Never… 7=Very often) **The scales are adapted from Ajzen, I. (2002, September).** ***Constructing a Theory of Planned Behavior Questionnaire.***
Perceived ease of use	Please indicate how much you agree with the following statements. ● I keep up with the latest technological developments in my areas of interest. ● I find that I have fewer problems than other people in making technology work for me.	7 points Likert scales (1=Strongly disagree… 7=Strongly agree)
Perceived usefulness	Please indicate how much you agree with the following statements. ● I think I would find Smart Speaker/Smart Personal Assistant to be easy to use. ● I think I would find it easy to get Smart Speaker Assistant to do what I want it to do. Developed from Preference for Technology survey- Classroom Edition	7 points Likert scales (1=Strongly disagree… 7=Strongly agree)
Perceived control	Please indicate how much you agree with the following statements. ● I believe I would have full control over the data I disclose to Smart Speaker Assistant. It is mostly up to me whether to disclose information to Smart Speaker Assistant.	7 points Likert scales (1=Strongly disagree… 7=Strongly agree)

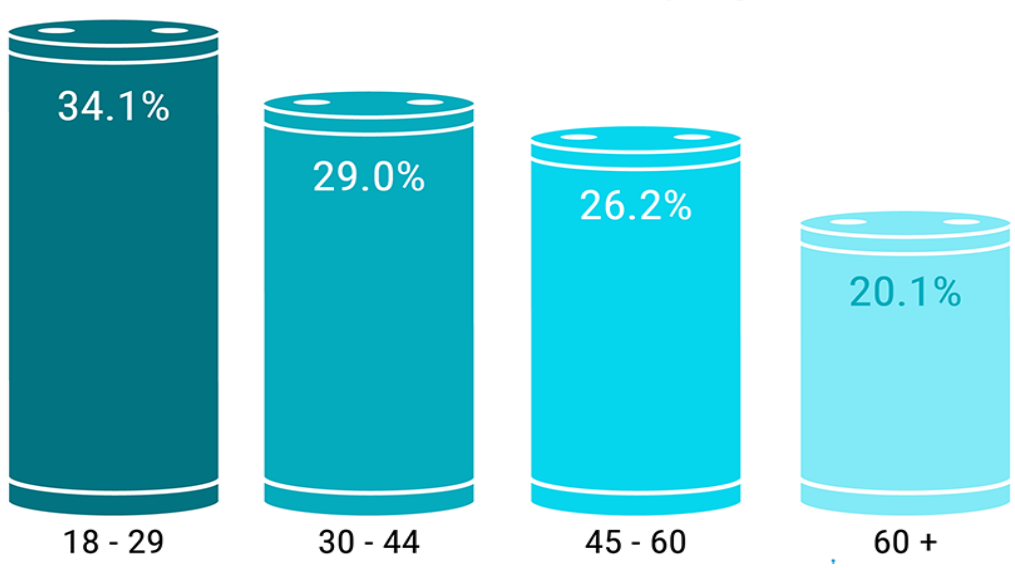
APPENDIX 5: SMART SPEAKER USE CASE FREQUENCY IN THE UNITED STATES IN JANUARY 2020



Source: Retrieved from Statista. (2022, March 28). *Main smart speaker uses cases in the U.S. 2020*. https://www.statista.com/statistics/994696/united-states-smart-speaker-use-case-frequency/

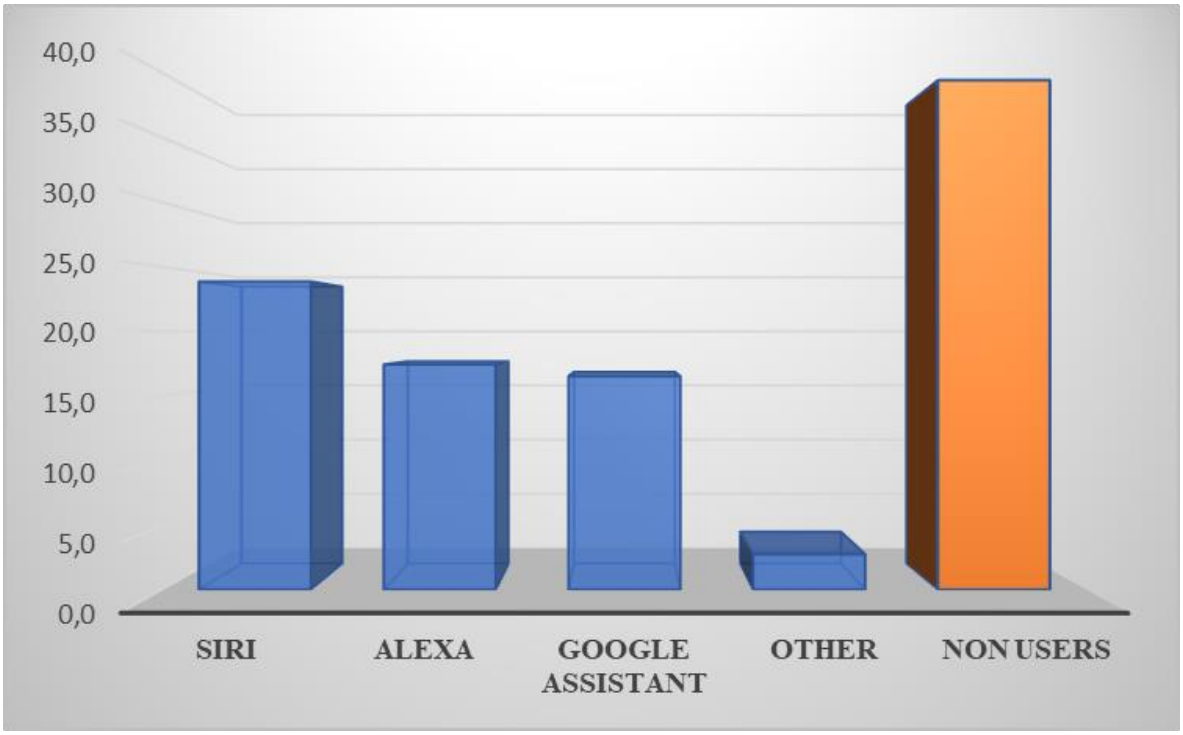
APPENDIX 6: SURVEY DISTRIBUTION CHANNEL

APPENDIX 7: SMART SPEAKER OWNERSHIP BY AGE GROUP IN 2019



Source: Retrieved from Kinsella, B. (2019, June 21). *Voice Assistant Demographic Data - Young Consumers More Likely to Own Smart Speakers While Over 60 Bias Toward Alexa and Siri*.

APPENDIX 8: SMART PERSONAL ASSISTANT OWNERSHIP BY BRAND



Source: Retrieved from the results of our AIA privacy investigation-survey (2022)

APPENDIX 9: MULTICOLINEARITY REDUCTION

IV	DV	Full model			Full model standardized		
		R^2	Coef	p	R^2	Coef	p
Perceived benefit (PB) [H2]	Intention disclosure	0,117	0,214	0,041	0,066	0,325	**0,027****

Notes: IV, independent variable; DV, dependent variables.

Source: Retrieved from the results of our AIA privacy investigation-survey (2022)

APPENDIX 10: ROBUSTNESS CHECK: BOOTSTRAP

IV	DV	Full model		
		R^2	Coef(SE)	p
Privacy Concern (PC)	Intention disclosure	0,122	-0,387 (0,095)	0,001***
Perceived benefit (PB)	Intention disclosure	0,038	0,244 (0,115)	0,038*
Privacy protection Awareness (PPA)	Intention disclosure	0,108	0,282 (0,072)	0,001***
Relationship Length (RL)	Intention disclosure	0,000	0,012 (0,087)	0,893
Privacy Concern (PC)	Actual disclosure	0,015	-0,089 (0,071)	0,205
Perceived benefit (PB)	Actual disclosure	0,000	-0,010 (0,070)	0,867
Information to privacy protection (IPP)	Actual disclosure	0,004	0,035 (0,048)	0,468
Relationship Length (RL)	Actual disclosure	0,136	-0,220 (0,049)	0,001***
Intention disclosure	Intention disclosure	0,06	0,161 (0,066)	0,024**
Main effect of the moderators				
PC*RL	Intention disclosure	0,126	0,026 (0,064)	0,655
PC*IPP	Intention disclosure	0,210	0,36 (0,001)	0,323

Notes: N= 1000. All independent variables are standardized. The coefficients of the control variables are omitted. R2 for PC*RL and PC*IPP explained the power of the overall predictors on intention disclosure (privacy concern, relationship length, PC*RL) and (privacy concern, information to privacy, PC*IPP) respectively. *p<0.05; **p<0.01; ***p<0.001.

APPENDIX 11: DISCRIMINANT VALIDITY

Variables	Mean	SD	1	2	3	4	5	6
1.Privacy Concern	5,31	1,296	**0.805**					
2.Perceived Benefit	5,64	1,149	-0,043	**0.721**				
3.Intention Disclosure	3,16	1,433	-,350**	,196*	**0.66**			
4.Actual Disclosure	2,47	0,945	-0,121	-0,013	,243*	**0.673**		
5.Information to Privacy Protection	3,65	1,667	-0,118	0,173	,328**	0,061	**0.905**	
6.Relationship Length	2,52	1,585	-0,171	0,095	0,014	-,368**	0,077	-

SD, Standard deviation. Diagonal elements (italic) are the square roots of AVE.
Off-diagonal elements are the correlations among constructs. *p<0.05; **p<0.01; ***p<0.001.

APPENDIX 12: MULTIPLE LINEAR REGRESSION WITH 4 STRUCTURAL MODELS

IV	DV	Full model with control variables				Model w/o control variables			
		MODEL 1	MODEL 2	MODEL 3	MODEL 4	MODEL1	MODEL 2	MODEL3	MODEL4
Privacy concern	Intention disclosure	*1,10* -0,339 (0,001) ***	*1,15* -0,338 (0,001) ***	1,14 -0,320 (0,000) ***	4,35 -0,36 (0,049) *	*1,00* -0,378 (0,000) ***	*1,042* -0,359 (0,000) ***	1,042 -0,327 (0,0003)***	4,08 -0,38 (0,032) *
Perceived benefit	Intention disclosure	*1,17* 0,17 (0,077)	*1,18* 0,19 (0,113)	1,20 0,188 (0,05) *	1,15 0,17 (0,077)	*1,002* 0,225 (0,045) *	*1,038* 0,177 (0,108)	1,082 0,16 (0,071)	1,045 0,15 (0,10)
Information to privacy protection	Intention disclosure		*1,16* 0,206 (0,012) **	*1,08* 0,271 (0,003) **	*1,10* 0,273 (0,003) **		*1,05* 0,233 (0,003) **	1,047 0,268 (0,003) **	1,054 0,268 (0,0031)**
Relationship length	Intention disclosure		*1,1* -0,059 (0,472)	1,105 -0,069 (0,45)	16,29 -0,165 (0,641)		*1,04* -0,069 (0,39)	*1,04* -0,082 (0,35)	*15,32* -0,19 (0,56)
PC*IPP	Intention disclosure			*1,06* 0,107 (0,233)				*1,05* 0,101 (0,252)	
PC*RL	Intention disclosure				*16,7* 0,108 (0,763)				*16,04* 0,126 (0,716)
Privacy concern	Actual disclosure	*1,1* -0,049 (0,493)	*1,15* -0,097 (0,162)			*1,001* -0,089 (0,208)	*1,04* -0,133 (0,05)		
Perceived benefit	Actual disclosure	*1,17* 0,061 (0,461)	*1,17* 0,056 (0,47)			*1,00* -0,015 (0,853)	*1,04* 0,005 (0,94)		
Information to privacy protection	Actual disclosure		*1,16* 0,039 (0,469)				*1,045* 0,039 (0,443)		
Relationship length	Actual disclosure		*1,10* -0,211 (0,000) ***				*1,040* -0,242 (0,000) ***		

Notes: IV, Independent Variable; DV, Dependent Variable; VIFs are the coefficients written in italic. p is written in bracket and the standardized coefficient is written without it.

Model 1: main predictors: privacy concern, perceived benefit disclosure

Model 1 with control variables: (R^2=0,203 for explaining intention R^2=0,114 for explaining actual disclosure)

Model 1 without control variables: (R^2=0,155 for explaining intention R^2=0,015 for explaining actual disclosure)

Model 2: main predictors: privacy concern, perceived benefit, information to privacy protection, relationship length

Model 2 with control variables: (R^2=0,239 for explaining intention R^2=0,231 for explaining actual disclosure)

Model 2 without control variables: (R^2=0,229 for explaining intention R^2= 0,176 for explaining actual disclosure)
Model 3: main predictors: privacy concern, perceived benefit, information to privacy protection, relationship length, PC*IPP, privacy concern* information to privacy protection
Model 3 with control variables: (R^2=0,250 for explaining intention)
Model 3 without control variables: (R^2=0,239 for explaining intention)
Model 4: main predictors: privacy concern, perceived benefit, information to privacy protection, relationship length, PC*RL, privacy concern* relationship length
Model 4 with control variables: (R^2=0,240 for explaining intention disclosure)
Model 4 with control variables: (R^2=0,239 for explaining intention disclosure).
The overall model with main factors and intention disclosure (DV) indicate good fit: CFI=0.92; TLI=0.9; RMSEA=0.07; CMIN/df=1,6 compared to the model with actual disclosure (DV) with CFI=0,81; TLI=0,77; RMSEA=0,106; CMIN/df=2,2).

APPENDIX 13: COVARIANCES

			Estimate	S.E.	p
PB	<-->	IPP	0,264	0,113	0,020*

Notes: SE, Standard error; PB, perceived benefit; IPP; Information to privacy protection. Dependent variable: Actual disclosure in the model. *p<0.05; **p<0.01; ***p<0.001.

			Estimate	S.E.	p
PB	<-->	IPP	0,267	0,114	0,019*
RL	<-->	PC	-0,523	0,159	0,001***

Notes: SE, Standard error; Main predictors: PC, privacy concern, PB, perceived benefit; IPP; Information to privacy concern, RL, relationship length. Dependent variable: Intention disclosure in the model. *p<0.05; **p<0.01; ***p<0.001.