Pacific Asia Journal of the Association for Information Systems

ISSN 1943-7544

Research Paper doi: 10.17705/1pais.15102 Volume 15, Issue 1 (2023)

Swaying Individuals' Privacy Concerns via Amplifying versus Diminishing Counter Argument

Nan (Tina) Wang[1,*], Louisa Rieger[2]

[1,*]Eastern Illinois University, USA, nwang@eiu.edu
[2]Eastern Illinois University, USA, louisa.rieger@gmx.de

Abstract

Background: *Though limited, research has found that individuals' privacy concerns could be swayed by counter argument. This study investigated the swaying influence of amplifying vs. diminishing argument (i.e., counter argument seeking to increase or decrease privacy concerns) on individuals' privacy concerns and the moderating influences of level of sensitivity and privacy-related knowledge.*

Method: *Data was collected using online survey and respondents were college students enrolled in a Midwestern university. 215 students participated in the survey, resulting in 180 completed responses; two factors (survey competition time and response consistency for reversely-coded items) were used to screen response quality and 90 responses were kept. Data was analyzed using univariate analysis.*

Results: *Results suggest that the swaying influence of counter argument depends on the level of sensitivity—the swaying influence is greater when individuals are presented with amplifying (diminishing) argument for a highly (less) sensitive issue/scenario. In addition, although the swaying influence is smaller for those with high privacy knowledge in general, it is not necessarily easier to sway those with low privacy knowledge. Instead, those with low privacy knowledge are more likely to get stuck or trapped in their existing privacy beliefs when facing privacy argument inconsistent with their existing beliefs, and are more likely to be provoked or stirred up when facing argument reinforcing their existing beliefs.*

Conclusion: *Findings suggest that when processing privacy argument, individuals show confirmation bias and tend to "go with their initial assessments". This is especially true for those with low privacy knowledge. When facing privacy related argument, individuals with low privacy knowledge behave the opposite of how magnets work—while magnets' opposite poles attract each other and similar poles repel, individuals with low privacy knowledge embrace argument consistent with their existing beliefs and repel/reject argument inconsistent with their existing beliefs.*

Keywords: Privacy Concern, Counter Argument, Swaying Influence, Awareness Motivation Capability Perspective.

This research article was submitted on September-2022 and under two revisions, accepted on January-2023.

Citation: Wang, N., & Rieger, L. (2023). Swaying Individuals' Privacy Concerns via Amplifying versus Diminishing Counter Argument. *Pacific Asia Journal of the Association for Information Systems, 15*(1), 29-55. https://doi.org/10.17705/1pais.15102

Introduction

> *In our daily lives, too many of us favor the comfort of conviction over the discomfort of doubt. We listen to opinions that make us feel good, instead of ideas that make us think hard. We see disagreement as a threat to our egos, rather than an opportunity to learn. We surround ourselves with people who agree with our conclusions, when we should be gravitating toward those who challenge our thought process. The result is that our beliefs get brittle long before our bones. We think too much like preachers defending our sacred beliefs, prosecutors proving the other side wrong, and politicians campaigning for approval…* (Publisher's description about the 2021 book *Think Again* by Adam Grant)

Individuals' privacy concerns and the impacts on intentions, attitudes, and behaviors (e.g., information disclosure) have received extensive attention (see Bélanger & Crossler, 2011; Kshetri, 2011; Mitchell & El-Gayar, 2022; Pavlou, 2011; Smith et al., 2011 for reviews). One interesting phenomenon related to privacy concerns is privacy paradox, which is the gap between individuals' concerns for privacy and their actual behaviors (see Barth & de Jong, 2017; Gerber et al., 2018; Kokolakis, 2017 for reviews). For example, individuals may claim they are very concerned about their privacy and yet do very little (or nothing) to protect it, or even worse, may trade their privacy for convenience or small benefits (e.g., a few dollars' savings). Existing research has identified several explanations for privacy paradox such as bounded rationality and learned helplessness (e.g., Bandara et al., 2020; Kokolakis, 2017). For example, repeated intrusion of privacy may make individuals feel that sacrificing privacy is the price they have to pay to use the technology (e.g., mobile app) and/or that they are powerless to change the situation (Shklovski et al., 2014).

Another possible explanation for privacy paradox, which has received limited attention, is that individuals' privacy concerns may change. Privacy paradox research that examined individuals' actual privacy-related behaviors (not just self-reported behavioral intention) often collected data on privacy concerns and on actual behaviors at separate points of time in order to eliminate response biases (e.g., Williams et al., 2019). For example, in their 3-week experiment testing privacy paradox in the context of mobile app use, Barth and colleagues (2019) collected data on general privacy concern in week 1, actual mobile app download and use in week 2, and post-use privacy concern in week 3; findings suggest that neither the general privacy concern (collected in week 1) nor the post-use privacy concern (collected in week 3) was related to the decision to download the app or not. An implicit assumption of such design (i.e., collecting privacy concerns and actual behaviors at separate points of time) is that individuals' privacy concerns remain unchanged between the two separate data collections. However, accumulated knowledge in psychology and privacy suggests that individuals' privacy concerns may change (e.g., Barth & de Jong, 2017; Mourey & Waldman, 2020; Srivastava & Rojhe, 2021).

Though limited, extant research has found that individuals' privacy concerns could be swayed when they are presented with counter argument (Baek, 2014). However, current (and very limited) research at the intersection of privacy paradox and counter argument viewed counter argument homogeneously and only compared the presence versus. (vs. hereafter) absence of counter argument. What remains to be investigated is whether the nature of counter argument may affect the swaying influence.

This study seeks to extend the current research at the intersection of privacy paradox and counter argument by distinguishing between privacy amplifying argument (i.e., argument seeking to increase individuals' privacy concerns) and privacy diminishing argument (i.e., argument seeking to reduce individuals' privacy concerns) to see if they differ in the swaying influence. In addition, we would like to understand what factors may moderate the swaying impact of amplifying vs. diminishing argument. This study asks the following questions:

https://aisel.aisnet.org/pajais/vol15/iss1/2
DOI: 10.17705/1pais.15102

Research question 1: Does amplifying vs. diminishing argument similarly or differently change individuals' privacy concerns?
Research question 2: What factors may moderate the above impact and how?

Understanding the above research questions may provide theoretical and practical values. Theoretically, this study may provide an important methodological contribution to the privacy paradox literature. If individuals' privacy concerns are (differently) swayed by amplifying vs. diminishing argument, researchers need to take this into consideration when designing their studies. Failing to do so may raise the question that the so-called gap between individuals' privacy concerns and their actual behaviors does not exist and is simply due to changes of individuals' privacy concerns. In addition, understanding moderators of the swaying influences may extend the currently limited research regarding the swaying influence of counter argument and clarify contingencies regarding the swaying influence.

Practically, understanding how (amplifying vs. diminishing) argument may change individuals' privacy concerns and the possible moderators could provide valuable insights for organizations across different sectors and industries (e.g., e-commerce, health care, and e-government). Take the monitoring of mobile phone data as an example. Despite the generally unfavorable attitude toward government collecting mobile phone data, individuals, during the COVID-19 pandemic, showed greater tolerance after knowing how monitoring mobile phone data helps with contact tracing and related issues such as quarantine enforcement; many individuals even voluntarily signed up to use related applications (apps) or websites and provided personal data to help with those issues (Fahim et al., 2020). In addition, understanding moderators could provide insights regarding "targeted" swaying influences (e.g., what kinds of individuals should be the focus target to achieve the biggest swaying influence) and regarding how to counteract undesired swaying influences (e.g., what can we do to reduce the swaying influence).

The remaining of the paper will be structured as follows. We first discuss related research on privacy paradox, counter argument and privacy concerns. Next, we introduce the theoretical basis, the awareness-motivation-capability perspective. Then, we discuss our hypotheses, data collection, and analysis, before presenting our results. Discussion, theoretical contributions, practical implications, limitations, and future research are provided in the end.

Literature Review

Privacy Paradox

Privacy paradox refers to the discrepancy between individuals' expressed privacy concerns and their actual behaviors (e.g., Barth & de Jong, 2017). While individuals generally show concerns about and interest in privacy protection, their privacy concerns often do not translate into actual privacy protection behaviors; on the contrary, individuals may trade their privacy in exchange for benefits such as personalized services and discounts (e.g., Barth & de Jong, 2017). For example, many insurance companies like State Farm provide customers the option to use Bluetooth beacons for driving monitoring, which tracks a wide range of driving behaviors and patterns such as speeding, braking, cornering and phone usage. Despite concerns about the large amount of data being tracked (and about the information that could be inferred from those tracked data, such as individuals' activity routine), many individuals voluntarily sign up to use those beacons in exchange for insurance discounts. Extant research has found the existence of privacy paradox across different contexts such as social media, social networking site, e-commerce/m-commerce, mobile app and health care (e.g., Bandara et al., 2020; Barth & de Jong, 2017; Barth et al., 2019; Fox, 2020; Liyanaarachchi, 2021; Massara et al., 2021; Xie et al., 2019).

Research has tried to explain privacy paradox. Barth and de Jong's (2017) review of the privacy paradox literature indicates that there are two primary explanations for the discrepancy between privacy concerns and actual behaviors: First, after conducting risk-benefit evaluations, individuals decide that the benefits of information disclosure outweigh the risks. Here, the risk-benefit evaluations could be rational or biased due to influences such as time constraint and immediate gratification. Second, due to reasons such as incomplete information and a lack of related knowledge (at both technical and legal levels), individuals may be unaware of and/or unable to calculate risks associated with information disclosure. As a result, individuals use benefits as "the sole reference point" (Barth & de Jong, 2017, p.1048) with little to no risk assessment.

So far, scholarly efforts examining privacy paradox held an implicit assumption that individuals' privacy concerns remain stable. Extant research often collected data on privacy concerns and on actual behaviors at separate time, with privacy concerns usually collected first and behaviors collected (often weeks/months) later (Barth et al., 2019; Williams et al., 2019). In fact, when discussing research limitations toward the end of their literature review, Barth and de Jong (2017) argued that "Privacy concerns seem to be highly situation-dependent and can be described as a fluent concept that changes over time. However, most studies have researched privacy as a stable concept..." (p. 1052). Their critique is also supported by the accumulated knowledge in the psychology and related literature, which suggests that individuals' privacy concerns are not stable and subject to influences like counter argument, as discussed below.

Swaying Influence of Counter Argument and Privacy Concern

Literature on persuasion and attitude change has long recognized the swaying influence of counter argument and factors that moderate the swaying influence (e.g., prior exposure to counter argument, source credibility, issue involvement) (e.g., Hass & Linder, 1972; McGuire, 1961; Park et al., 2007; Petty & Cacioppo, 1979; Rydell et al., 2007; Srivastava & Rojhe, 2021). Meanwhile, individuals' privacy concerns have been found to be highly superficial and subject to many influences such as social expectations and moods (Barth & de Jong, 2017; Wakefield, 2013; Williams et al., 2017). For example, research found that positive mood-inducing website features may increase individuals' tendency to give the benefit of the doubt, hence reducing individuals' privacy concerns (Wakefield, 2013).

Surprisingly, limited research has examined the possible swaying influence of counter argument on individuals' privacy concerns. One exception is Baek (2014), which, via sampling respondents from South Korea, found that individuals' privacy concerns could be swayed after being presented with counter argument. However, Baek (2014) only examined the presence vs. absence of counter argument, and it is unclear whether different types of counter argument—amplifying vs. diminishing argument—have similar or different swaying impact. To better understand the swaying influence of counter argument and possible moderators of the swaying influence, we turn to the awareness-motivation-capability perspective.

The Awareness-Motivation-Capability Perspective

The awareness-motivation-capability (AMC) perspective suggests there are three drivers of behavioral actions, i.e., awareness, motivation, and capability (e.g., Chen, 1996; Chen et al., 2007). Awareness represents an individual's perception of the environment, motivation refers to an individual's desire to act, and capability focuses on an individual's ability of undertaking the action. In essence, for individuals to undertake an action, they need to be aware of it, be motivated to do it, and have the capability needed to undertake said action.

The AMC perspective, which has been used to examine issues at both organizational level (e.g., Shamsuzzaman et al., 2018; Shi et al., 2020; Stadtler & Lin, 2017) and individual level

https://aisel.aisnet.org/pajais/vol15/iss1/2
DOI: 10.17705/1pais.15102

(e.g., Bloodgood & Chen, 2021; Chen et al., 2018), is a general framework and the three drivers have different manifestations in different contexts or studies. For example, in the literature on firms' competitive tension, awareness has been manifested as action visibility (Chen & Miller, 1994) and firm size or operational capacity (e.g., Chen & Miller, 1994; Chen et al., 2007); motivation has been manifested as market commonality (Chen, 1996) and rival's attack volume (Chen et al., 2007); capability has been manifested as resource similarity (Chen, 1996) and contest capability (Chen et al., 2007).

In addition, while early AMC research (e.g., Chen, 1996) focused on main effects of the three behavioral drivers, subsequent research (by Chen and by other researchers) included interaction effects. Chen and colleagues (2007) argued that "In addition to the independent effect each awareness-motivation-capability component has on perceived competitive tension there are likely to be interaction effects…" (p.106). Empirical research has confirmed both main effects of the three drivers (e.g., Chen et al., 2018; Stadtler & Lin, 2017) as well as interaction effects between awareness and motivation and between awareness and capability (e.g., Chen et al., 2007; Shi et al., 2020) in leading to behavioral changes.

The AMC perspective is appropriate for our research, as it has been successfully applied to understand similar issues such as individuals' compliance with security policies (e.g., Chen et al., 2018), knowledge adoption (Sussman & Siegal, 2003), and knowledge acquisition (Bloodgood & Chen, 2021). For example, Bloodgood and Chen (2021) applied the AMC framework to understand knowledge acquisition and argued that for individuals to acquire knowledge, they need to be aware of the knowledge, and to have the motivation and capability to acquire it.

Hypothesis Development

In this section, we apply the AMC perspective to understand the swaying influence of (amplifying vs. diminishing) argument on individuals' privacy concerns. In line with Bloodgood and Chen's (2021) application of the AMC perspective as discussed above, we argue that for individuals to change their privacy concerns, they need to be aware of possible "flaws" in their initial privacy concerns, and are motivated and capable of adjusting their privacy concerns. Specifically, the presence of (amplifying or diminishing) argument helps individuals recognize possible "flaws" in their initial privacy concerns, corresponding to the awareness component of the AMC perspective. In addition, such swaying influence is moderated by individuals' motivation and capability of processing counter argument, manifested as the level of sensitivity of collected information and as individuals' privacy-related knowledge respectively. Figure 1 illustrates our research model.

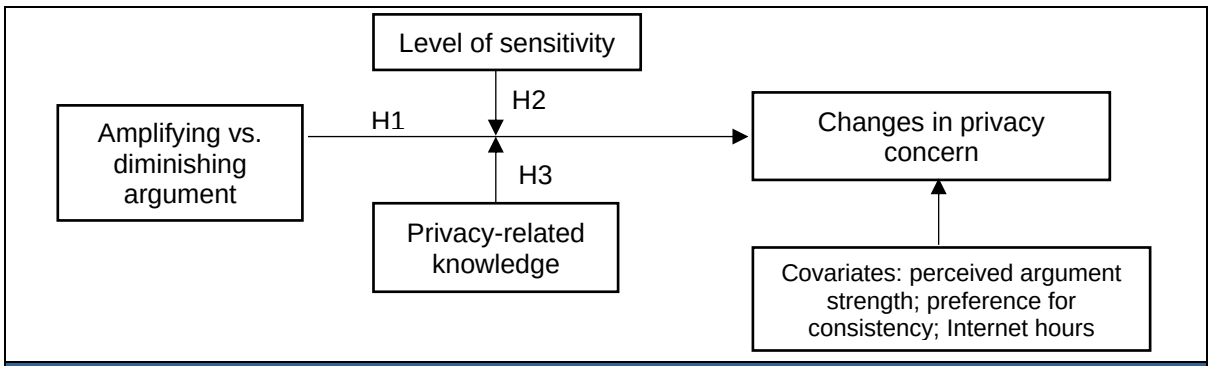

Figure 1 – Research Model

Awareness: Amplifying vs. Diminishing Counter Argument

For individuals to change their opinions, either about privacy or about other issues, an important prerequisite is they are aware of counter argument challenging their current beliefs (e.g., Chen, 1996). Psychology research on persuasion and attitude change has recognized that different types of argument (e.g., cognitive- vs. affective-based argument, Keer et al., 2013; Millar & Millar, 1990; Petty et al., 2003; Rosselli et al., 1995) may have different impacts on attitude change. When it comes to privacy concerns, individuals are frequently exposed to privacy-related argument. Some argument seeks to increase individual's privacy concerns (or amplifying argument) while other seeks to decrease individual's privacy concerns (or diminishing argument). In this study, we seek to understand whether amplifying vs. diminishing argument has similar or different swaying influence.

Extant literature in psychology and behavioral economics and recent research on privacy suggests that individuals often show cognitive biases in information processing (e.g., Dinev et al., 2015; Waldman, 2020). For example, research found that emotions may affect the formation of privacy concerns (Li et al., 2008). Amplifying argument, which tends to cause stronger emotional reactions and trigger individuals' tendency for risk aversion (Ariely et al., 2005; Tversky & Kahneman, 1981, 1991), may have a stronger swaying influence as compared to diminishing argument. Hence, we suspect

> H1: Amplifying argument leads to bigger changes in individuals' privacy concerns than diminishing argument.

Motivation: Level of Sensitivity

Level of sensitivity (or information sensitivity) refers to "the potential loss associated with the disclosure of that information" (Mothersbaugh et al., 2012, p.77), where the potential loss could be "psychological (e.g., loss of self-concept due to embarrassment), physical (e.g., loss of life or health), or material (e.g., loss of financial or other assets…)" (p.77). Level of sensitivity may affect individuals' concern or involvement regarding privacy (e.g., Brough & Martin, 2020; Mitchell & El-Gayar, 2022), corresponding to the motivation component of the AMC perspective.

Individuals tend to stick with their original opinions and are less likely to attend to (let alone be persuaded by) counter argument when they do not care much about the issue (e.g., McGuire, 1961). We suspect level of sensitivity may moderate the swaying influence of counter argument by increasing individuals' concern with the issue and consequently the cognitive efforts they allocate to process argument. The higher the level of sensitivity, the more individuals care about the privacy issue (Brough & Martin, 2020; Mothersbaug et al., 2012), the more cognitive efforts they allocate for argument processing (Petty & Cacioppo, 1986; Petty et al., 1981; Ratneshwar & Chaiken, 1991), and consequently the greater the swaying influence. Our hypothesis can find support in the extant literature. For example, Sussman and Siegal's (2003) study on knowledge adoption found that the level of involvement in a topic may amplify the impact of argument quality on attitude change; the greater individuals' level of involvement, the stronger the impact of argument quality on attitude change. Hence, we argue

> H2: The swaying influence described in H1 is moderated by level of sensitivity. The higher the level of sensitivity, the greater the swaying influence (i.e., bigger changes in privacy concerns).

https://aisel.aisnet.org/pajais/vol15/iss1/2
DOI: 10.17705/1pais.15102

Capability: Privacy-related Knowledge

Privacy-related knowledge, corresponding to the capability component of the AMC perspective, may also moderate the swaying influence of counter argument. Research indicates that when individuals are knowledgeable about something, their opinions tend to be more stable and less likely to be swayed (e.g., Baek, 2014; Converse, 1964; Simpson et al., 2008; Zaller, 1992). For example, psychology research on yielding (i.e., opinion change) and persuasion found that individuals with high knowledge are less likely to change their opinions (or be persuaded), because they are more confident with their original opinions, can conduct critical evaluation of and identify flaws from others' argument, can assemble rebuttals for others' argument, and etc (e.g., Petty et al.,1997; Rhodes & Wood,1992; Wood, 1982; Wood et al., 1985; Wood et al., 1995).

The IS literature also provides indirect support for the lower influenceability of individuals with high knowledge. For example, research on electronic word-of-mouth (e.g., product/service reviews) found that others' reviews have a smaller influence on the purchase intention of individuals with high knowledge/expertise related to the product/service, because they are more confident with their own opinions/assessments (Cheung et al., 2012; Park & Kim, 2008).

Overall, accumulated knowledge in both psychology and IS literature suggests that individuals with high knowledge are less likely to change opinion (or be persuaded) by counter argument. Hence, we suspect that the swaying influence of (amplifying or diminishing) argument is likely to be stronger (lower) for those with low (high) privacy-related knowledge.

> H3: The swaying influence described in H1 is moderated by individuals' privacy-related knowledge. The lower individuals' privacy-related knowledge, the greater the swaying influence (i.e., bigger changes in privacy concerns).

Method

Data Collection

Survey and Sample

Data was collected using an online survey, which proceeded as follows (Figure 2). One place worthy of clarification is regarding the initial message (step 2 in Figure 2) and the subsequent amplifying vs. diminishing argument (step 4 in Figure 2). Take the Fitbit scenario as an example. The initial message talks about basic features of Fitbit such as tracking workouts and location and time related to users' activities. It also briefly mentions some information that could potentially be "inferred" from tracked data, such as when users are likely to be at a certain place (e.g., gym). Subsequent diminishing argument discusses the great emphasis that companies (behind health apps like Fitbit) place on protecting health data due to their legal and ethical obligations, companies' heavy investment in data security technologies and experts, mandatory and regular employee training, and encryption and de-individualization of user data. Even in the incidence of data breach, de-individualization of user data would make it almost impossible to tell which data belongs to which user; subsequent amplifying argument, however, first mentions that a study of 60 different health apps found that none of them followed best practices for informing user about privacy. Very often, users do not know what they are agreeing to when accepting terms and conditions. Then, it raises the suspicion that those apps are likely to be selling user data in order to make a profit. Lastly, it argues that even if companies promise to de-identify user data, it is relatively easy to identify users through methods such as cross-indexing.

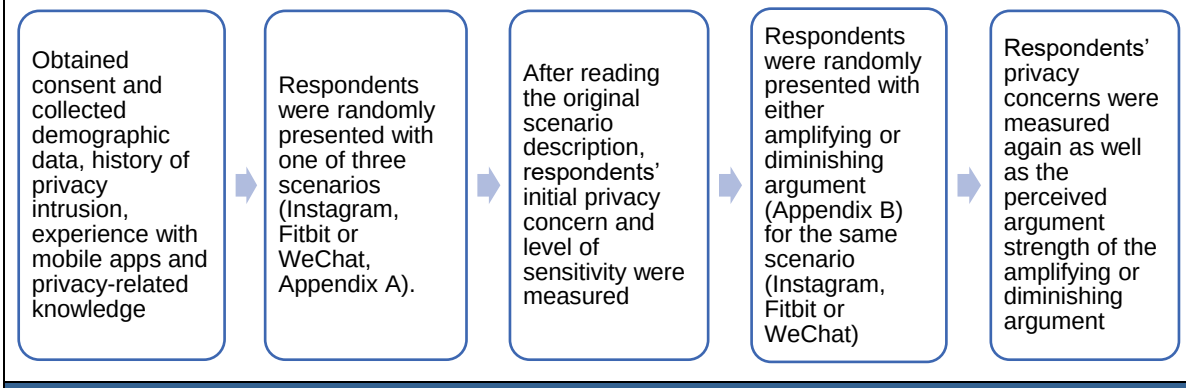

Figure 2 – Survey Data Collection Steps

Respondents were undergraduate students enrolled at a public Midwestern university in the US. 215 students participated in the survey, resulting in 180 complete responses. We then eliminated potential problematic responses by considering two indicators of response quality, i.e., survey completion time and response consistence for reversely coded items. Specifically, we excluded responses from surveys submitted within 7 minutes after starting or if response differences for reversely coded items are greater than 2 (out of 7-point Likert scales). Both indicators provide consistent conclusions regarding response quality. In the end, 90 responses were kept. Demographic information is summarized in Table 1.

Table 1 – Respondent Demographics

Demographics	Mean	Std. Dev
Age	19.87	2.774
Gender (male=1, female=2)	1.60	0.492
Year in college	2.07	1.281
Privacy intrusion (no prior experience =1, prior experience =2)	1.51	0.503

Construct

Independent variable. The independent variable is the presence of amplifying vs. diminishing counter argument and is manipulated in this study. As described before, respondents, after being first presented with 1 of 3 randomly selected scenario, were subsequently and randomly presented with either amplifying or diminishing argument for that scenario (Appendix B).

Dependent variable. The dependent variable is changes in individuals' privacy concerns. Privacy concerns were measured twice, first after respondents were presented with the initial message (step 3 in Figure 2) and again after they were presented with either amplifying or diminishing argument (step 5 in Figure 2). The absolute difference between the two scores reflects changes in individuals' privacy concerns. Measurement items were adapted from existing scales and are summarized in Appendix C.

Moderator. One of the two moderators is privacy-related knowledge, which was measured by adapting Hargittai and Hsieh (2012), as in Appendix C. The other moderator is level of sensitivity, and we handled it in two different ways: We measured it by asking "In your opinion, how sensitive is the information collected by [Instagram/Fitbit/WeChat] (e.g. [browsing behavior/location data/payment information]?"; we also tried to manipulate it via the three scenarios, i.e., Instagram, Fitbit, and WeChat, as discussed below.

Existing research (e.g., Kokolakis, 2017; Mothersbaugh et al., 2012) focuses on the sensitivity level of different types of information (e.g., contact information, general financial information, media usage information) and suggests that different types of information trigger varying levels

https://aisel.aisnet.org/pajais/vol15/iss1/2
DOI: 10.17705/1pais.15102

of privacy concerns (Brough & Martin, 2020; Mothersbaugh et al., 2012). Individuals, for example, are generally more comfortable with disclosing age than with disclosing address or income. However, websites and mobile apps often collect multiple information such as address, phone number, and social contacts. The extant literature, to the best of our knowledge, does not provide a convincing and comprehensive ranking of the overall sensitivity level of all information collected by different websites and mobile apps. In this study, we picked three mobile apps (i.e., Instagram, Fitbit, and WeChat) that likely vary in the level of sensitivity considering their different focuses (e.g., Matt et al., 2019; Mitchell & El-Gayar, 2022) and that are appropriate for our respondents. It is of both theoretical and practical values to see how the three scenarios differ in the overall level of sensitivity and in the swaying influence of amplifying vs. diminishing argument.

Control variable. Control variables include Internet hours (i.e., the number of hours individuals spend on Internet per day), preference for consistency, i.e., "a dispositional preference for or against consistent responding" (Cialdini et al., 1995, p. 319), and perceived argument strength. Both preference for consistency and perceived argument strength were measured by adapting existing scales (Appendix C).

Manipulation Check and Construct Reliability

We first conducted a manipulation check to see whether our amplifying (diminishing) argument indeed increased (reduced) individuals' privacy concerns, i.e., changes in privacy concerns are statistically different from zero. Two separate one-sample t-tests showed that our manipulation worked considering our small sample ($p=0.01$ for amplifying argument, $p=0.09$ for diminishing argument). We also checked for the level of sensitivity of the three scenarios using ANOVA. Results show a significant difference ($p=0.002$) among the three scenarios. Specifically, the WeChat scenario was perceived to have the lowest level of sensitivity, while the Fitbit scenario was perceived to have the highest level of sensitivity.

Common Method Bias

Common method bias was tested using Harman's single factor method. Exploratory factor analysis was implemented and unrotated results showed that the first factor only explained 17.196% of the total variance. As such, common method bias was not a concern.

Construct Reliability and Validity

For construct reliability, we looked at both composite reliability (CR) and Cronbach's α values (Table 2). Cronbach's α values range from 0.715 to 0.915, above the recommended threshold of 0.7; CR values range from 0.812 to 0.943, also exceeding the recommended threshold of 0.7. Together, they show adequate construct reliability.

Both convergent validity and discriminant validity tests were used to assess construct validity. For convergent validity, we look at factor loading and average variance extracted (AVE). A recent guidance for factor loading cut-offs is provided by Tabachnick and Fidell (2007), specifically, 0.32 (poor), 0.45 (fair), 0.55 (good), 0.63 (very good) or 0.71 (excellent). All factor loadings (Table 2) exceed 0.63. In addition, AVE values (Table 2) range from 0.521 to 0.805, exceeding the cutoff value of 0.5. For discriminant validity, Table 3 shows that the square root of AVE values (diagonal and italic) are greater than the correlation between any pair of measured constructs (bottom off-diagonal values), suggesting adequate discriminant validity (Fornell & Larcker, 1981).

Table 2 – Construct Reliability and Convergent Validity Assessment

Construct	Item	Factor Loading	Cronbach's Alpha	Composite Reliability (CR)	Average Variance Extracted (AVE)
Privacy concern (PC)*	PC1	0.922	0.914	0.943	0.805
	PC2	0.809			
	PC3	0.917			
	PC4	0.935			
Perceived argument strength (PAS)	PAS1	0.893	0.915	0.911	0.721
	PAS2	0.890			
	PAS3	0.717			
	PAS4	0.883			
Preference for consistency (PFC)	PFC2	0.787	0.715	0.812	0.521
	PFC3	0.764			
	PFC5	0.692			
	PFC8	0.634			
Privacy-related knowledge (PRK)	PRK 1	0.745	0.85	0.887	0.531
	PRK 4	0.777			
	PRK 6	0.641			
	PRK 7	0.633			
	PRK 8	0.761			
	PRK 9	0.834			
	PRK 10	0.685			

**privacy concern was collected twice. The above statistics are from 2nd data collection. We also tried using 1st data collection and statistics are consistent. For example, Cronbach's Alpha is 0.833 using 1st privacy concern data, still above the recommended threshold.*

Table 3 – Discriminant Validity Assessment

Construct	PC	PAS	PFC	PFK
Privacy concern (PC)	*0.8972*			
Perceived argument strength (PAS)	0.0154	*0.8491*		
Preference for consistency (PFC)	0.0755	0.195*	*0.7218*	
Privacy-related knowledge (PFK)	0.0158	-0.0003	-0.0106	*0.7287*

(Diagonal and italic: square root of AVE; off-diagonal: correlation)

Data Analysis and Results

Descriptive Statistics is summarized in Table 4. Data was standardized before being analyzed and hypotheses were tested using univariate analysis.

We argue that amplifying argument may lead to a bigger change in privacy concerns as compared to diminishing argument (H1). Results (left side of Table 5) show that H1 was not supported. We also hypothesize that the swaying influence of amplifying vs. diminishing argument is moderated by level of sensitivity (H2) and by privacy-related knowledge (H3). Results (right side of Table 5) show a significant interaction between amplifying vs. diminishing argument and level of sensitivity and a non-significant interaction with privacy-related knowledge, supporting H2 and failing to support H3.

https://aisel.aisnet.org/pajais/vol15/iss1/2
DOI: 10.17705/1pais.15102

Table 4 – Descriptive Statistics

	Mean	Std. Dev	Privacy change	Amplifying vs. Diminishing argument	Scenario	Level of sensitivity	Privacy-related knowledge	Internet hours	Preference for consistency
Privacy change	0.599	0.614	1						
Amplifying vs. Diminishing argument	0.549	0.500	-0.115	1					
Scenario	1.978	0.816	0.143	-0.133	1				
Level of sensitivity	2.451	1.336	0.138	0.158	-.276**	1			
Privacy-related knowledge	3.500	1.351	-.189*	0.062	0.048	-0.049	1		
Internet hours	4.861	2.662	0.086	-0.157	-0.016	-0.116	0.070	1	
Preference for consistency	5.044	0.911	-0.101	-0.047	-0.100	0.086	-0.022	0.112	1
Perceived argument strength	4.849	0.965	-0.051	-0.137	-0.163	0.094	0.001	0.046	.195*

*: p<0.05, **: p<0.01, ***: p<0.001
The above statistics are based on unstandardized data

Table 5 – Analysis Results

Results for H1		**Results for H2-H3**	
Amplifying vs. Diminishing **(H1)**	0.141	Amplifying vs. Diminishing	0.290+
Diminishing argument as the comparison base group			
Scenario =Instagram	-0.336	Scenario =Instagram	-0.333+
Scenario=Fitbit	-0.208	Scenario=Fitbit	-0.249
The WeChat Scenario as the comparison base group			
Level of sensitivity	0.158+	Level of sensitivity	-0.004
Privacy-related knowledge	-0.132+	Privacy-related knowledge	-0.219*
Internet hours	0.089	Internet hours	0.037
Preference for consistency	-0.077	Preference for consistency	-0.035
Perceived argument strength	-0.032	Perceived argument strength	-0.049
		Amplifying vs. diminishing * Level of sensitivity **(H2)**	**0.462****
		Amplifying vs. diminishing * Privacy-related knowledge **(H3)**	0.123

+: p<0.1, *: p<0.05, **: p<0.01, ***: p<0.001

To better illustrate the interactional effect for H2, we present two figures below, corresponding to the two treatments of level of sensitivity (i.e., measured and manipulated) used in this study. Figure 3 shows that the swaying influence was greater when the level of sensitivity is higher, and the biggest swaying influence (i.e., changes in privacy concerns) happened when respondents were presented with amplifying messages that were also perceived to be highly sensitive, supporting H2. Figure 4 shows that amplifying argument had the biggest swaying influence in the Fitbit scenario, which was perceived by respondents to have the highest level of sensitivity, while diminishing argument had the biggest swaying influence in the WeChat scenario, which was perceived by respondents to have the lowest level of sensitivity. This non-linear swaying influence of amplifying vs. diminishing argument on privacy concerns once again shows the importance of distinguishing the different types of counter argument in future research.

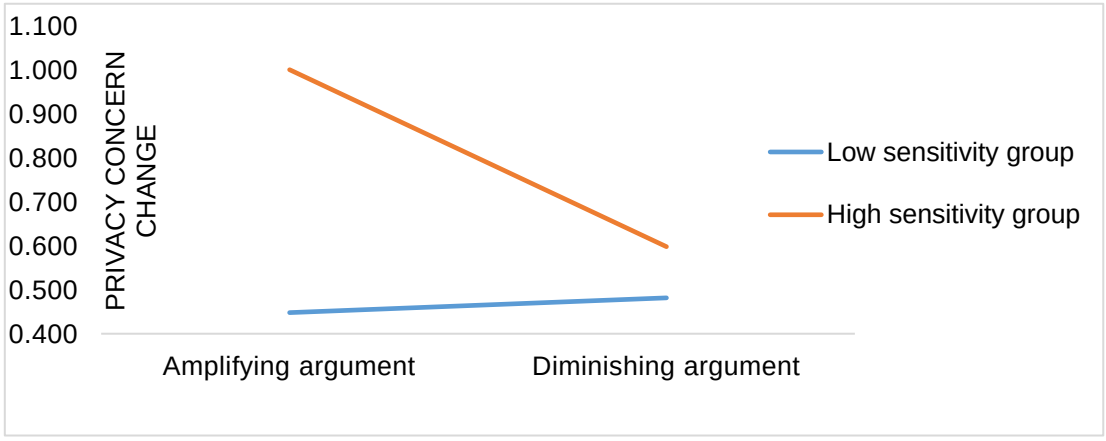

Figure 3 – 2-way Interaction between Amplifying vs. Diminishing Argument and Level of Sensitivity

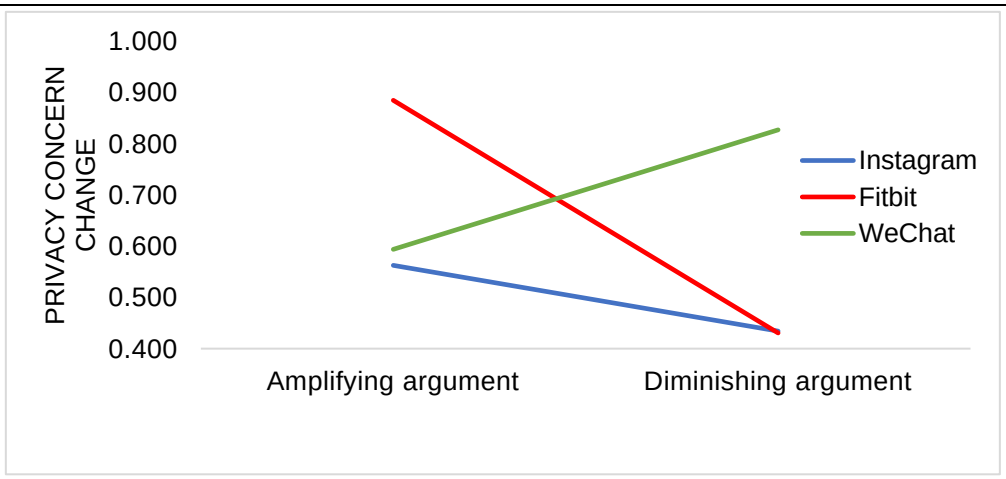

Figure 4 – 2-way Interaction between Amplifying vs. Diminishing Argument and Scenario

The interaction between amplifying vs. diminishing argument and privacy-related knowledge was non-significant, failing to support H3. Upon further investigation, we found an almost significant (p=0.082) 3-way interaction among amplifying vs. diminishing argument, privacy-based knowledge, and scenario (Figure 5). Figure 5 shows that, for individuals with low privacy knowledge (top section of Figure 5), amplifying argument had the greatest swaying influence on individuals' privacy concerns in the Fitbit scenario (with highest level of sensitivity) and the smallest swaying influence in the WeChat scenario (with lowest level of sensitivity);

https://aisel.aisnet.org/pajais/vol15/iss1/2
DOI: 10.17705/1pais.15102

diminishing argument, however, showed the opposite pattern, showing greatest swaying influence in the WeChat scenario (with lowest sensitivity) and smallest swaying influence in the Fitbit scenario (with highest sensitivity), similar to that of the Instagram scenario.

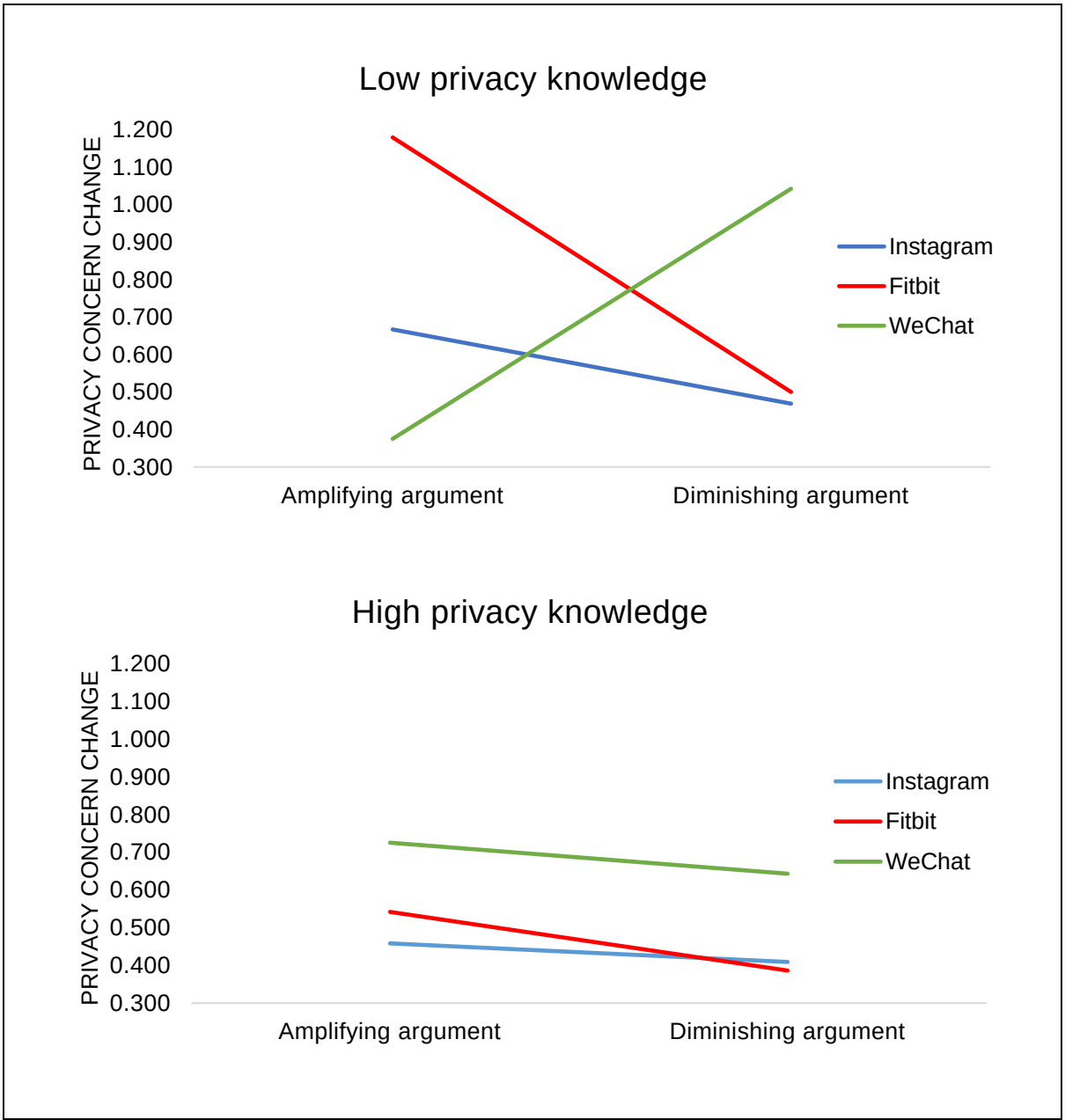

Figure 5 – 3-way Interaction among Amplifying vs. Diminishing Argument, Privacy-related Knowledge and Scenario

For individuals with high privacy knowledge, amplifying vs. diminishing argument showed similar swaying influences, as can be seen from the almost horizontal lines on the bottom section of Figure 5. In addition, the swaying influence is higher in the WeChat scenario than in the other two. The smaller swaying influence for Instagram and Fitbit could be due to respondents' greater familiarity with the two mobile apps.

Discussion

Utilizing the AMC perspective as the underlying theoretical basis, we examined the possible swaying influence of amplifying vs. diminishing argument on individuals' privacy concerns and factors (i.e., level of sensitivity and privacy-related knowledge) moderating the swaying influence. Findings suggest that, contrary to our expectation, amplifying argument did not have a greater swaying influence as compared to diminishing argument. Instead, the extent of the swaying influence depended on the level of sensitivity and more importantly, the interaction between amplifying vs. diminishing argument and the level of sensitivity. Specifically, individuals' privacy concerns showed a bigger change when the level of sensitivity was high, especially when individuals were also presented with amplifying argument.

The interaction between amplifying vs. diminishing argument and scenario provides interesting insights (Figure 4). First, when presented with either amplifying or diminishing argument, individuals showed the smallest change in privacy concerns in the Instagram scenario (with medium level of sensitivity). One possible explanation is that our respondents are very familiar with social media apps like Instagram. As a result, their privacy concerns regarding Instagram are more set and less likely to be swayed by either amplifying or diminishing argument.

Second and more interestingly, Figure 4 shows that amplifying argument caused the biggest change in privacy concerns in the Fitbit scenario (with the highest level of sensitivity) and smallest change in the WeChat scenario (with the lowest level of sensitivity); meanwhile diminishing argument caused the biggest change in the WeChat scenario (with the lowest level of sensitivity) and the smallest change in the Fitbit scenario (with the highest level of sensitivity). That is, when the issue or situation is perceived to be high (low) in sensitivity, argument trying to reduce (increase) individuals' privacy concerns are likely to make a very small difference while argument trying to increase (decrease) individuals' privacy concerns are likely to have a big impact. In a word, individuals seem to discount (embrace) privacy argument that are inconsistent (consistent) with their initial assessments—This is consistent with the psychology literature on *confirmation bias* (or *my-side bias*), i.e., the tendency individuals have to seek or interpret information supporting their beliefs (e.g., expectations, hypotheses) and to avoid or reject information contradicting their beliefs (see Klayman, 1995; Nickerson, 1988 for reviews).

We also suspected that privacy-related knowledge may moderate the swaying influence such that the swaying influence is stronger for those with low privacy knowledge. We found a non-significant interaction between amplifying vs. diminishing argument and privacy-related knowledge; further examination revealed an almost significant 3-way interaction among amplifying vs. diminishing argument, privacy-related knowledge, and scenario (Figure 5), which provides additional insights regarding the confirmation bias mentioned above.

The top section of Figure 5 suggests that individuals with low privacy-related knowledge are more likely to discount (embrace) privacy argument that are inconsistent (consistent) with their initial assessments. If the issue or scenario is perceived to be high in sensitivity (i.e., Fitbit), amplifying argument caused the biggest change while diminishing argument caused the smallest change. In contrast, if the issue or scenario is perceived to be low in sensitivity (i.e., WeChat), diminishing argument caused the biggest change while amplifying argument caused the smallest change. Comparing the top and the bottom sections of Figure 5, we can see that although individuals with high privacy knowledge show small change in privacy concerns in general (i.e., across scenarios and when presented with either amplifying or diminishing argument), those with low privacy knowledge are *only* willing to change their privacy concerns when the argument is consistent with their initial assessments and are reluctant to change when the argument is inconsistent. That is, the confirmation bias discussed previously is largely due to individuals with low privacy knowledge—Just as the old saying goes, individuals with low privacy knowledge tend to "only hear what they want to hear" when it comes to privacy related argument.

https://aisel.aisnet.org/pajais/vol15/iss1/2
DOI: 10.17705/1pais.15102

Theoretical Contributions

This study provides several theoretical contributions to the privacy concern and privacy paradox literature. First, findings show that individuals' privacy concerns can indeed be swayed by counter argument, confirming Baek's findings (based on a South Korean sample). Hence, future research on privacy paradox should take this into consideration when designing research to examine the gap between privacy concerns and actual privacy-related behaviors. Ignoring this may raise the question that the so-called "gap" does not exist and simply reflects individuals' changes of privacy concerns due to the influence of counter argument (and possibly other factors).

Second, our findings suggest that it is important to distinguish between amplifying and diminishing argument and to consider possible moderators of the swaying influence. Although the main effect of amplifying vs. diminishing argument is non-significant, the significant interaction between amplifying vs. diminishing argument and level of sensitivity suggests that it is still necessary to distinguish between amplifying vs. diminishing argument and that attempts to increase (decrease) privacy concern work better when the issue/situation is highly (less) sensitive. Future research is encouraged to continue investigating under what conditions could (amplifying or diminishing) argument has the greatest (smallest) swaying influence on individuals' privacy concerns.

Third, our findings also suggest that future research on privacy concern should pay more attention to the possible confirmation bias individuals have when interpreting (and possibly seeking) privacy-related argument. The 3-way interaction (Figure 5) shows that confirmation bias is greater for those with low privacy knowledge. Those with low privacy knowledge are more closed-minded and more likely to get stuck or trapped in their existing privacy beliefs when facing privacy argument *inconsistent* with their existing beliefs, and are also more likely to be provoked or stirred up when facing argument *reinforcing* their existing beliefs. That is, when facing privacy-related argument, individuals with low privacy knowledge behave the opposite of how magnets work—while magnets' opposite poles attract each other and similar poles repel (e.g., north poles attract south poles but repel north poles), individuals with low privacy knowledge embrace argument consistent with existing beliefs and repel/reject argument inconsistent with existing beliefs.

Practical Implications

Attempts to influence others, if not done appropriately, may backfire, as "what doesn't sway people may strengthen their beliefs. Much as a vaccine inoculates the physical immune system against a virus, the act of resistance fortifies the psychological immune system. Refuting a point of view produces antibodies against future attempts at influence, making people more certain of their own opinions and more ready to rebut alternatives" (Grant, 2021, p.1). This study offers practical implications regarding swaying others' privacy concerns.

First, the significant interaction between amplifying vs. diminishing argument and level of sensitivity suggests that attempts to increase (decrease) privacy concern work better when the issue/situation is highly (less) sensitive. That is, when trying to influence others' privacy concerns about a certain issue, individuals should "go with the flow, not against." Understanding this may help individuals better target their swaying attempts.

Second, when attempting to influence others, individuals should be aware of (and hopefully be prepared for) the possible confirmation bias that targets may possess. While individuals with high privacy knowledge have more stable privacy concerns (and hence show smaller swaying influence of counter argument) as we expected, those with low privacy knowledge, contrary to our expectation, are not necessarily easier to be swayed. Instead, those with low

privacy knowledge are found to show greater confirmation bias when processing privacy-related argument, "only hearing what they want to hear". Hence, individuals seeking to influence others need to be aware of (and hopefully prepared for) the fact that targets with low privacy knowledge are more closed-minded when presented with counter argument.

Third and of particular importance to the Asia Pacific region, this paper emphasizes the importance of understanding and considering the swaying possibility of individuals' privacy concerns. Unlike the European Union (EU) region that has shared privacy law, the Asia Pacific region's privacy regulations are diverse and (frequently) changing. According to Deloitte's Asia Pacific Privacy Guide 2020-2021 (Deloitte, 2020), some countries like Bangladesh do not have a comprehensive privacy law and instead have only very narrow/specific regulations (e.g., Bangladesh's Digital Security Act of 2018); countries that have privacy law often have their own "flavors". In addition, privacy regulations in the Asia Pacific region are (frequently) changing. For example, many countries in the Asia Pacific region have recently amended or are amending their privacy regulations in order to obtain a favorable 'adequacy decision' from the EU, to reduce restrictions on cross-border data transfer between their businesses and businesses in the EU. Moreover, there have been several high-profile data breaches in the Asia Pacific region in recent years, for example, Singapore's 2018 data breach that affected 1.5 million patients, including Prime Minister Lee Hsien Loong and several ministers. As a result, individuals' awareness of and concerns about privacy have significantly increased in the region (Deloitte, 2020). Hence, it becomes increasingly important for organizations and governments to understand individuals' privacy concerns and to sway their privacy concerns when appropriate. For example, during the COVID-19 pandemic, many countries in the Asia Pacific region adopted contact tracing technologies (e.g., Japan's COCOA, New Zealand's NZ COVID, South Korea's Co100, and Singapore's TraceTogether and SafeEntry). Those technologies often collect lots of personal and health data, raising individuals' privacy concerns. It is crucial for governments to understand individuals' privacy concerns and to know how to sway their privacy concerns, to facilitate adoption and proper use of those technologies.

The Asia Pacific region is also characterized by different stages of economic development, rates of technology adoption, levels of education and cultures. For example, countries in the Asia Pacific region vary significantly on power distance, one of the six culture dimensions by Hofstede (Hofstede, 2001; Hofstede et al., 2010), with countries like Malaysia scoring the highest on power distance while some like New Zealand scoring among the lowest. Those culture differences, according to extant research, likely lead to differences in individuals' privacy concerns (e.g., Lu et al., 2018; Wu et al., 2012). In addition, the different stages of technology adoption and levels of education among Asian Pacific countries suggest that there are likely cross-country differences in privacy-related knowledge, one of the moderators examined in this paper. Last but not least, there are likely cross-country differences in the perceived sensitivity level of the same data. Take health data as an example. In the US, health data is protected under Health Insurance Portability and Accountability Act (HIPAA), and our US-based sample viewed health data (collected by Fitbit) as highly sensitive. However, health data may not be viewed as highly sensitive in certain Asian Pacific countries that prioritize providing adequate and affordable health care to citizens. Individuals' perception of the sensitivity level may also change. For example, after Singapore's several health data breaches in recent years (including the above-mentioned high-profile breach affecting its prime minister), individuals' perception regarding the sensitivity level of health data might change.

In summary, when trying to understand and influence individuals' privacy concerns, organizations and governments in the Asian Pacific region need to take into consideration many factors, such as the country's legal environment, technology adoption and education level, and potential cross-cultural differences in individuals' perceptions and attitudes toward privacy.

https://aisel.aisnet.org/pajais/vol15/iss1/2
DOI: 10.17705/1pais.15102

Limitations and Future Research Directions

One limitation of this study is the sample population and therefore the generalizability of our findings. Since data was collected from a small sample of undergraduate students in the US, it is possible that findings may vary when using a different sample. Future research testing our research model using different and bigger sample population is encouraged. Another limitation is the single-item measurement of level of sensitivity. Future research using more reliable multi-item measurement is encouraged. Finally, this study included only three scenarios (i.e., Instagram, Fitbit, and WeChat) considering our sample. There are many other types of apps and devices widely used nowadays that may raise potential privacy concerns (e.g., smart thermostats and cameras monitoring household schedule and activities). Future research testing different scenarios is strongly encouraged.

Conclusion

This study investigated the swaying influence of amplifying vs. diminishing argument on individuals' privacy concerns and the moderating impacts of level of sensitivity and privacy-related knowledge. Results suggest that the swaying influence of amplifying vs. diminishing argument depends on the level of sensitivity—the swaying influence is greater when individuals are presented with amplifying (diminishing) argument for a highly (less) sensitive issue/scenario. In addition, this study found that individuals with low privacy knowledge also show greater confirmation (or my-side) bias when processing privacy related argument. While individuals with high privacy knowledge show small changes in privacy concerns in general, those with low privacy knowledge are only willing to change, in fact greatly change, their privacy concerns when presented with argument consistent with their initial assessments. If the presented argument is inconsistent with their initial assessments, individuals with low privacy knowledge are reluctant to change. That is, when facing privacy related argument, individuals with low privacy knowledge behave the opposite of how magnets work—while magnets' opposite poles attract each other and similar poles repel, individuals with low privacy knowledge embrace argument consistent with existing beliefs and repel/reject argument inconsistent with existing beliefs.

References

Ariely, D., Huber, J., & Wertenbroch, K. (2005). When do losses loom larger than gains? *Journal of Marketing Research, 42*(2), 134-138.

Baek, Y. M. (2014). Solving the privacy paradox: A counter argument experimental approach. *Computers in Human Behavior*, *38*, 33-42.

Baek, Y. M., Kim, E. M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior*, *31*, 48-56.

Bandara, R., Fernando, M., & Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services*, *52*, 101947.

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.

Barth, S., de Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*, 55-69.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1041.

Bloodgood, J. M., & Chen, A. N. (2021). Preventing organizational knowledge leakage: The influence of knowledge seekers' awareness, motivation and capability. *Journal of Knowledge Management*, *26*(9), 2145-2176.

Bright, L. F., Lim, H. S., & Logan, K. (2021). "Should I Post or Ghost?": Examining how privacy concerns impact social media engagement in US consumers. *Psychology & Marketing*, *38*(10), 1712-1722.

Brough, A. R., & Martin, K. D. (2020). Critical roles of knowledge and motivation in privacy research. *Current Opinion in Psychology, 31*, 11-15.

Chen, M. J. (1996). Competitor analysis and interfirm rivalry: Toward a theoretical integration. *Academy of Management Review, 21*(1), 100-134.

Chen, X., Chen, L., & Wu, D. (2018). Factors that influence employees' security policy compliance: An awareness-motivation-capability perspective. *Journal of Computer Information Systems, 58*(4), 312-324.

Chen, M. J., & Miller, D. (1994). Competitive attack, retaliation and performance: An expectancy-valence framework. *Strategic Management Journal*, *15*(2), 85-102.

Chen, M. J., Su, K. H., & Tsai, W. (2007). Competitive tension: The awareness-motivation-capability perspective. *Academy of Management Journal*, *50*(1), 101-118.

Cheung, C. M. K., Xiao, B., & Liu, I. L. B. (2012). The impact of observational learning and electronic word of mouth on consumer purchase decisions: The moderating role of consumer expertise and consumer expertise and consumer involvement. In *45th Hawaii International Conference on System Sciences*, Maui, HI, USA

Cho, H., Lee, J. S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior, 26*(5), 987-995.

https://aisel.aisnet.org/pajais/vol15/iss1/2
DOI: 10.17705/1pais.15102

Cialdini, R. B., Trost, M. R., & Newsom, J. T. (1995). Preference for consistency: The development of a valid measure and the discovery of surprising behavioral implications. *Journal of Personality and Social Psychology, 69*(2), 318-328.

Converse, P. E. (1964). The nature of belief systems in mass publics In D. E. Apter (Ed.), *Ideology and Discontent* (pp. 206-261). New York: The Free Press.

Deloitte. (2020). *The Asia Pacific Privacy Guide 2020-2021*. Deloitte. https://www2.deloitte.com/ph/en/pages/risk/articles/asia-pacific-privacy-guide.html

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

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.

Fahim, K., Kim, M. J., & Hendrix, S (2020, May). *Cellphone monitoring is spreading with the coronavirus. So is an uneasy tolerance of surveillance.* The Washington Post. https://www.washingtonpost.com/world/cellphone-monitoring-is-spreading-with-the-coronavirus-so-is-an-uneasy-tolerance-of-surveillance/2020/05/02/56f14466-7b55-11ea-a311-adb1344719a9_story.html

Fornell, C., & Larcker, D. F., (1981). Evaluating structural equations with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Fox, G. (2020). "To protect my health or to protect my health privacy?" A mixed-methods investigation of the privacy paradox. *Journal of the Association for Information Science and Technology, 71*(9), 1015-1029.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226-261.

Grant, A. (2021). *Think Again: The Power of Knowing What You Don't Know*. New York: Penguin Publishing Group.

Hargittai, E., & Hsieh, Y. P. (2012). Succinct survey measures of web-use skills. *Social Science Computer Review, 30*(1), 95-107.

Hass, R. G., & Linder, D. E. (1972). Counterargument availability and the effects of message structure on persuasion. *Journal of Personality and Social Psychology, 23*(2), 219-233.

Hofstede, G. (2001). *Culture's Consequences: Comparing values, Behaviors, Institutions, and Organizations Across Nations*. Thousand Oaks, CA: Sage Publications.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and Organizations: Software of the Mind* (3rd ed.). New York, NY: McGraw-Hill Professional.

Hornikx, J., Weerman, A., & Hoeken, H. (2022). An exploratory test of an intuitive evaluation method of perceived argument strength. *Studies in Communication Sciences, 22*(2), 311-324.

James, T. L., Wallace, L., Warkentin, M., Kim, B. C., & Collignon, S. E. (2017). Exposing others' information on online social networks (OSNs): Perceived shared risk, its determinants, and its influence on OSN privacy control use. *Information & Management, 54*(7), 851-865.

Keer, M., van den Putte, B., Neijens, P., & de Wit, J. (2013). The influence of affective and cognitive argument on message judgement and attitude change: The moderating effects of meta-bases and structural bases. *Psychology & Health*, *28*(8), 895-908.

Klayman, J. (1995). Varieties of confirmation bias. *Psychology of Learning and Motivation*, *32*, 385-418.

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

Kshetri, N. (2011). Privacy and security aspects of social media: Institutional and technological environment. *Pacific Asia Journal of the Association for Information Systems, 3*(4), 1-20.

Li, H., Sarathy, R., & Zhang, J. (2008). The role of emotions in shaping consumers' privacy beliefs about unfamiliar online vendors. *Journal of Information Privacy and Security, 4*(3), 36-62.

Liyanaarachchi, G. (2021). Managing privacy paradox through national culture: Reshaping online retailing strategy. *Journal of Retailing and Consumer Services, 60*, 102500.

Lu, Q. S., Pattnaik, C., Xiao, J., & Voola, R. (2018). Cross-national variation in consumers' retail channel selection in a multichannel environment: Evidence from Asia-Pacific countries. *Journal of Business Research, 86*, 321-332.

Martin, M. M., Staggers, S. M., & Anderson, C. M. (2011). The relationships between cognitive flexibility with dogmatism, intellectual flexibility, preference for consistency, and self-compassion. *Communication Research Reports, 28*(3), 275-280.

Matt, C., Becker, M., Kolbeck, A. & Hess, T. (2019). Continuously healthy, continuously used? – A thematic analysis of user perceptions on consumer health wearables. *Pacific Asia Journal of the Association for Information Systems, 11*(1), 108-132

Massara, F., Raggiotto, F., & Voss, W. G. (2021). Unpacking the privacy paradox of consumers: A psychological perspective. *Psychology & Marketing, 38*(10), 1814-1827.

McGuire, W. J. (1961). Resistance to persuasion conferred by active and passive prior refutation of the same and alternative counterargument. *The Journal of Abnormal and Social Psychology, 63*(2), 326-332

Millar, M. G., & Millar, K. U. (1990). Attitude change as a function of attitude type and argument type. *Journal of Personality and Social Psychology, 59*(2), 217-228.

Min, J., & Kim, B. (2014). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. *Journal of the Association for Information Science and Technology, 66*(4), 839-857.

Mitchell, D. R., & El-Gayar, O. F. (2022). Privacy and online social networks: A systematic literature review of concerns, preservation, and policies. *Pacific Asia Journal of the Association for Information Systems, 14*(4), 1-25.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research, 15*(1), 76-98.

Mourey, J. A., & Waldman, A. E. (2020). Past the privacy paradox: The importance of privacy changes as a function of control and complexity. *Journal of the Association for Consumer Research, 5*(2), 162-180.

Nail, P. R., Correll, J. S., Drake, C. E., Glenn, S. B., Scott, G. M., & Stuckey, C. (2001). A validation study of the preference for consistency scale. *Personality and Individual Differences, 31*(7), 1193-1202.

Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology, 2*(2), 175-220.

Park, D. H., & Kim, S. (2008). The effects of consumer knowledge on message processing of electronic word-of-mouth via online consumer reviews. *Electronic Commerce Research and Applications, 7*(4), 399-410.

https://aisel.aisnet.org/pajais/vol15/iss1/2
DOI: 10.17705/1pais.15102

Park, H. S., Levine, T. R., Kingsley Westerman, C. Y., Orfgen, T., & Foregger, S. (2007). The effects of argument quality and involvement type on attitude formation and attitude change: A test of dual-process and social judgment predictions. *Human Communication Research, 33*(1), 81-102.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go?. *MIS Quarterly, 35*(4), 977-988.

Petty, R. E., & Cacioppo, J. T. (1979). Issue involvement can increase or decrease persuasion by enhancing message-relevant cognitive responses. *Journal of Personality and Social Psychology, 37*(10), 1915-1926.

Petty, R. E., & Cacioppo, J. T. (1986). *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*. New York: Springer-Verlag.

Petty, R. E., Cacioppo, J. T., & Goldman, R. (1981). Personal involvement as a determinant of argument-based persuasion. *Journal of Personality and Social Psychology, 41*(5), 847-855.

Petty, R. E., Fabrigar, L. R., & Wegener, D. T. (2003). Emotional factors in attitudes and persuasion. In R. J. Davidson, K. R. Scherer, & H. H. Goldsmith (Eds.), *Handbook of affective sciences* (pp.752-772). New York, NY: Oxford University Press.

Petty, R. E., Wegener, D. T., & Fabrigar, L. R. (1997). Attitudes and attitude change. *Annual Review of Psychology, 48*(1), 609-647.

Ratneshwar, S., & Chaiken, S. (1991). Comprehension's role in persuasion: The case of its moderating effect on the persuasive impact of source cues. *Journal of Consumer Research*, *18*(1), 52-62.

Rhodes, N., & Wood, W. (1992). Self-esteem and intelligence affect influenceability: The mediating role of message reception. *Psychological Bulletin, 111*(1), 156-171.

Rosselli, F., Skelly, J. J., & Mackie, D. M. (1995). Processing rational and emotional messages: The cognitive and affective mediation of persuasion. *Journal of Experimental Social Psychology, 31*(2), 163-190.

Rydell, R. J., McConnell, A. R., Strain, L. M., Claypool, H. M., & Hugenberg, K. (2007). Implicit and explicit attitudes respond differently to increasing amounts of counter-attitudinal information. *European Journal of Social Psychology, 37*(5), 867-78

Shamsuzzaman, M., Jahan, S. M., & Aman, M. A. U. (2018). Revisiting the awareness–motivation–capability (amc) model of competitive dynamics: An augmented-AMC framework. *The Business & Management Review, 9*(4), 515-527.

Shi, W., Connelly, B. L., Hoskisson, R. E., & Ketchen Jr, D. J. (2020). Portfolio spillover of institutional investor activism: An awareness–motivation–capability perspective. *Academy of Management Journal*, *63*(6), 1865-1892.

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Toronto, ON, Canada.

Simpson, P. M., Siguaw, J. A., & Cadogan, J. W. (2008). Understanding the consumer propensity to observe. *European Journal of Marketing, 42*(1/2), 196-221

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-1015.

Srivastava, S., & Rojhe, K. C. (2021). Attitude formation and attitude change: A social psychological perspective. In B. Christiansen, & H. C. Chandan (Eds), *Handbook of Research on Applied Social Psychology in Multiculturalism* (pp.1-28). IGI Global.

Stadtler, L., & Lin, H. (2017). Moving to the next strategy stage: Examining firms' awareness, motivation and capability drivers in environmental alliances. *Business Strategy and the Environment, 26*(6), 709-730.

Sussman, S. W., & Siegal, W. S. (2003). Informational influence in organizations: An integrated approach to knowledge adoption. *Information Systems Research, 14*(1), 47-65.

Tabachnick, B. G., & Fidell L. S. (2007). *Using Multivariate Statistics* (5th ed.). Pearson Education Inc. New York: Allyn and Bacon.

Tversky A, & Kahneman D. (1981). The framing of decisions and the psychology of choice. *Science, 211*(4481), 453-458.

Tversky A, & Kahneman D. (1991). Loss aversion in riskless choice: A reference-dependent model. *The Quarterly Journal of Economics, 106*(4), 1039-1061.

Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems, 22*(2), 157-174.

Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology, 31*, 105-109.

Williams, M., Nurse, J. R. C., & Creese, S. (2017). Privacy is the boring bit: User perceptions and behaviour in the internet-of-things. In *2017 15th Annual Conference on Privacy, Security and Trust (PST),* Calgary, AB, Canada.

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

Wood, W. (1982). Retrieval of attitude-relevant information from memory: Effects on susceptibility to persuasion and on intrinsic motivation. *Journal of Personality and Social Psychology, 42*(5), 798-810.

Wood, W., Kallgren, C. A., & Preisler, R. M. (1985). Access to attitude-relevant information in memory as a determinant of persuasion: The role of message attributes. *Journal of Experimental Social Psychology, 21*(1), 73-85.

Wood, W., Rhodes, N., & Biek, M. (1995). Working knowledge and attitude strength: An information-processing analysis. In R. E. Petty & J. A. Krosnick (Eds), *Attitude Strength: Antecedents and Consequences* (pp.283-313). Lawrence Erlbaum Associates, Inc. Hillsdale, NJ: Erlbaum.

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.

Xie, W., Fowler-Dawson, A., & Tvauri, A. (2019). Revealing the relationship between rational fatalism and the online privacy paradox. *Behaviour & Information Technology, 38*(7), 742-759.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 798-824.

Zaller, J. R. (1992). *The Nature and Origins of Mass Opinion*. Cambridge University Press: New York.

Zhao, X., Strasser, A., Cappella, J. N., Lerman, C., & Fishbein, M. (2011). A measure of perceived argument strength: Reliability and validity. *Communication Methods and Measures, 5*(1), 48-75.

https://aisel.aisnet.org/pajais/vol15/iss1/2
DOI: 10.17705/1pais.15102

Appendix A – Initial Scenario (1 of the following 3 randomly presented)

Scenario A: Instagram

Social media platforms such as Instagram often gather large amounts of user data in order to personalize advertising. On Instagram, a user's search history, time spent on a specific post or interaction with friends are all collated and analyzed. In addition, third parties (mostly Websites that have an interest in selling their product) may monitor user behavior such as browsing behavior, location and keyboard inputs by the implementation of cookies (i.e., a small tracking program). By using different algorithms, Instagram is able to predict users' interests and influences their purchases. The ads users received are targeted with such accuracy, that some users suspect that Instagram listen to their daily conversations via the microphone of their phone.

Scenario B: Fitbit

Health and fitness apps are among the most popular apps in the App Store. They can track your workouts, guide you through a meditative session or remind you to take your medicine. While making life a lot more convenient for the user, this type of app also collects a lot of user data. An example for an all-around Fitness App is Fitbit. Paired with a fitness tracker (often a watch) the app tracks steps, workouts, weight (if paired with the Fitbit scale) and sleep. Many apps have an integrated workout tracker, that tells you how long your workout lasted or how many calories you burned. When you go for a walk, run or bike ride, often times the data collected includes distance which can be measured through the use of GPS. From this location-based data it is easy to determine where you live and your regular workout routine, as well as the times when you are not at home or when you are likely to be at a certain place, such as your preferred running loop or the gym.

Scenario C: Multi-purpose app WeChat

WeChat is a Chinese mobile app developed by Tencent. It is also known as China's "app for everything" or as a "super app" because of its wide range of functions and mini programs (e.g., food take-out, train reservation). It is by far the most used app in the Chinese market as it erased the need for any other app. Through WeChat you can pay a friend, make reservations, book a ride or even a doctor's appointment. In some cities, it is even possible to request a citizenship card over the app. Because of its popularity, many western companies, such as Venmo or Uber are looking at their Chinese counterpart for inspiration or to copy its features.

Despite the convenience of a super App like WeChat, there are some concerns regarding privacy that arise with it. Having individuals' data in one single place allows Tencent, the company that owns WeChat, to know almost everything about its users. This gives them an unpredictable amount of power that should not be underestimated. And since WeChat has no competitors in China, there are no alternative apps on the market that would make privacy a priority. In recent years, many IT experts around the world have raised concerns about Tencent's practices on data collection, sharing and security.

Video: https://www.youtube.com/watch?v=VAesMQ6VtK8 (1:35 – 3:55 min)

Appendix B – Subsequent Amplifying vs. Diminishing Argument

Presentation of privacy concern amplifying vs. diminishing argument

Scenario A: Instagram (1 of the following 2 randomly presented)

1. **Scenario A_1: Diminishing argument**
   While sometimes users are surprised by how well personalized advertising predicts their needs and desires, it is groundless to conclude that social media platforms like Instagram listen to our conversations through our phones. Many people, in contrast, would argue that Instagram is not listening to people for the purpose of personalized advertising because doing so is impossible, ineffective and inefficient. Below are some of their argument.
   - Impossible from a technical standpoint: The sheer amount of audio files that would have to be recorded and sent to Instagram represent an unrealistic number. A study from researches at Northeastern University found no evidence of audio files being transmitted from the phones.
   - Problem of distinguishing who says what: It would be impossible to single out different individuals in a conversation or in a group setting.
   - Cost: It would be far too expensive to gather and analyze that much data. Instead, there are other more cost-effective and efficient ways. Data, for example, can be sourced from masses of similar individuals (in terms of gender, age, education, etc.) to help figure out what individuals might like. Hence, even if you personally have never googled or spoken of a product or service, algorithms can figure out what might be on your mind based on information gather from those like you.
2. **Scenario A_2: Amplifying argument**
   Many Instagram users have reported to receive ads on products/services they have never "mentioned" to an electronic device, such as googling for it or viewing it on a shopping site. In most cases those personalized ads are very specific in terms of brand, color and other features. For example, it is reported that someone (say Jim) had a random five-minutes conversation with his cousin about an uncommon product during a hiking trip—before that, Jim has never googled it, shared some ideas about it, or wrote/liked it on any digital platform. Yet, the next morning after the hiking trip, that particular product (and model) mentioned during the conversation pops up in an ad on his Instagram feed. There are very few explanations as to how this is possible other than that Instagram (installed on our smart phones) listens to our conversations.

Scenario B: Fitbit (1 of the following 2 randomly presented)

1. **Scenario B_1: Diminishing argument**
   Apps like Fitbit help users to reach their fitness and health goals. It is a convenient all-in-one app that promotes healthy living in every aspect, by sending reminders to move or by motivating users to follow a specific diet. Keeping up a healthy lifestyle used to require a lot of self-discipline but is now more attainable for a large portion of the population. People who are more fit and who engage in regular physical activities have a higher life-expectancy. Apps like Fitbit therefore contribute to forming a healthier society.
   Since the data those apps collect are health related, they are considered to be highly sensitive. Companies behind this type of app are legally and ethically obligated to keep the data secured. As a result, user data privacy is a priority for them. They heavily invest in data security by hiring competent Cyber Security experts as well as keeping their information safety precautions at the highest standard. Not only do they keep their technology updated, but all employees that could potentially deal with user data have

https://aisel.aisnet.org/pajais/vol15/iss1/2
DOI: 10.17705/1pais.15102

to take part in mandatory data protection trainings on a regular basis. In addition to all these preventive measures, collected data is encrypted and de-identified (i.e., user identity and the other data are separated). Hence, even in the incidence of data breach/leakage, it would be (almost) impossible to tell which data belongs to which user.

2. **Scenario B_2: Amplifying argument**
   A study looking at 60 different health apps found that none of them followed best practices for informing users about privacy. In other words, users rarely know what they are agreeing to or worse, some apps do not even have a privacy policy to begin with. Realistically, the apps that are free to use have to make a profit somehow and unfortunately it is often by selling user data to third parties. Even if a company promises to de-identify data (i.e., user identity and the other data are separated), it is relatively easy to identify users by cross-indexing the data with other information available on the Internet. By collecting personal health information, third parties become experts about your life. They know how much you sleep, what you eat, how much you weigh and even where you live.

Scenario C: WeChat (1 of the following 2 randomly presented)

1. **Scenario C_1: Diminishing argument**
   Having all functions in one place is convenient and easy. It is also a better option with regard to privacy protection. Rather than giving one's data to many different companies (with varying resources and capabilities related to security), only one company (i.e., Tencent) owns those user data such as contacts (or friends) and purchases. And Tencent is at a significantly better position when it comes to protecting user's data and ensuring only authorized parties are able to access certain information. While a Chinese smartphone user might only have a single app on his/her phone, a peer living in the US might be using:
   - Uber to find a ride
   - iMessage to text friends
   - Venmo to send money
   - Doordash to order food

   Both the American and the Chinese users are able to use the same kinds of services, yet WeChat enables Chinese users to enjoy the services in a safer and far more convenient way.
2. **Scenario C_2: Amplifying argument**
   Below is some additional information regarding privacy issues in WeChat:
   a) Data collection policy
      As stated in WeChat's privacy policy, the following data is being collected regularly:
      - log data such as search terms, profiles visited, and content that had been viewed within the app
      - communication metadata such as call times, duration, and location information
      - text messages and contact books and user location

   b) Security practices
      Since the app does not use end-to-end encryption (like other messaging apps do), anyone with access to WeChat's servers is able to read messages. In addition, WeChat setting gives users limited option to control over their privacy. Countries like India have debated whether or not they should ban WeChat for its possibility in collecting too much personal data.
   c) Data sharing (or selling) practice
      It is not surprising that the data collected by WeChat could be used for personalized advertising and marketing purposes. In addition, rumors exist that the vast amount of data collected is also shared with the Chinese government.

Appendix C – Construct Measurement

Appendix C – Construct Measurement			
Construct	**Measurement Items (7-point Likert scales)**		**Reference**
Privacy concern (PC)	1. I am concerned that the information I submit on the Internet could be misused. 2. When I shop on-line, I am concerned that the credit card information can be stolen while being transferred on the Internet. 3. I am concerned about submitting information on the Internet because of what others might do with it. 4. I am concerned about submitting information on the Internet because it could be used in a way I did not foresee.		Bright et al., 2021; Cho et al., 2010; Dinev & Hart, 2004; James et al., 2017; Min & Kim, 2014; Xu et al., 2011
Perceived argument strength (PAS)	1. The above statement is believable. 2. The above statement is convincing. 3. The argument helped me feel confident about my knowledge regarding privacy issues. 4. Overall, how much do you agree or disagree with the statement? 5. *Is the above statement regarding privacy concern a strong or weak argument?*		Baek, 2014; Hornikx et al., 2022; Zhao et al., 2011
Preference for consistency (PFC)	*1. Even if my attitudes and actions seemed consistent with one another to me, it would bother me if they did not seem consistent in the eyes of others.* 2. I want to be described by others as a stable, predictable person. 3. Admirable people are consistent and predictable. *4. The appearance of consistency is an important part of the image I present to the world.* 5. I don't like to appear as if I am inconsistent. *6. I dislike people who are constantly changing their opinions.* *7. It is important to me that others view me as a stable person.* 8. I make an effort to appear consistent to others. *9. I'm uncomfortable holding two beliefs that are inconsistent.*		Cialdini et al., 1995; Martin et al., 2011; Nail et al., 2001
Privacy-related knowledge (PRK)	Privacy-related understanding of the following items:		Baek et al., 2014; Hargittai & Hsieh, 2012
	1. Advanced Search *2. Tagging* *3. PDF* 4. Spyware *5. Wiki*	6. JPG 7. Weblog 8. Cache 9. Malware 10. Phishing	
Note: Items in *italic* were dropped due to poor construct reliability and/or validity			

https://aisel.aisnet.org/pajais/vol15/iss1/2
DOI: 10.17705/1pais.15102

About the Authors

Nan (Tina) Wang is an Associate Professor in Management Information Systems (MIS) at Eastern Illinois University. She received her PhD in MIS from the University of Oklahoma. Her research interests include innovation adoption and implementation, computer-mediated communication, affect and affective social processes, managerial cognition, electronic commerce and online community. She has published at journals such as Information & Management, Information and Organization, and Journal of Computer Information Systems. She has also worked as associate editor and mini-track chair for conferences such as ICIS and AMCIS, and has served as a reviewer for journals such as MISQ and ISR.

Louisa Rieger received her Bachelor's degree in MIS from Eastern Illinois University, a Master's degree in Data Science from Ludwig-Maximilians-Universität München, and a Master's degree in Business Analytics from the University of Georgia. Her research interest focuses on privacy-related issues.