# Swaying Individuals’ Privacy Concerns Through Amplifying vs. Diminishing Counter Arguments: An Awareness-Motivation-Capability Perspective

Louisa F. Rieger
*Lumpkin School of Business*, louisa.rieger@gmx.de

Tina Wang
*Eastern Illinois University*, nwang@eiu.edu

# Swaying Individuals' Privacy Concerns Through Amplifying versus. Diminishing Counter Arguments: An Awareness-Motivation-Capability Perspective

*Completed Research*

**Louisa Rieger**
Eastern Illinois University
louisa.rieger@gmx.de

**Nan (Tina) Wang**
Eastern Illinois University
nwang@eiu.edu

## Abstract

Individuals' privacy concern has been found to be swayed by counter arguments. This study investigated the swaying influence of amplifying vs. diminishing arguments (i.e., counter arguments that seek to increase or decrease privacy concerns) on individuals' privacy concerns and the moderating impact of level of sensitivity and privacy-related knowledge. Data was collected using online survey and respondents were college students enrolled in a Midwest university. Results suggest that the swaying influence depends on the level of sensitivity—the greatest swaying influence happens when individuals are presented with amplifying arguments for a highly sensitive issue. In addition, the swaying influences are smaller for individuals with high privacy knowledge; for those with low privacy knowledge, however, the swaying influence is stronger when the arguments are consistent (as compared to inconsistent) with their initial assessments. In a word, individuals with low privacy knowledge show greater cognitive bias when processing privacy related arguments.

### Keywords

Privacy concern, counter arguments, swaying influence, amplifying arguments, diminishing arguments, level of sensitivity, privacy-related knowledge.

## Introduction

Individuals' concern for privacy and its impact on people's intention, attitudes and behaviors (e.g., intention to disclose information) has been researched abundantly (see Bélanger and Crossler, 2011; Pavlou 2011; Smith, Dinev and Xu, 2011 for reviews). One interesting phenomenon related to privacy concern is privacy paradox, which is the gap between individuals' concerns for privacy and their actual behaviors (Barth and Jong 2017). For example, individuals may claim that they are very concerned about their privacy, and yet do very little (or nothing) to protect their personal data, or even worse, trade their personal data for convenience or small benefits (e.g., a few dollars' saving). Existing research has identified potential explanations for privacy paradox such as bounded rationality and learned helplessness (e.g., Bandaraa, Fernandoa and After, 2020; Kokolakis, 2017).

Another possible explanation, which has received limited attention, is that individuals' privacy concerns may change. Most studies on privacy paradox collected individuals' privacy concerns and their actual behaviors at separate points of time in order to eliminate biases. For example, researchers may collect data on individuals' current privacy concerns and on privacy-related behaviors that occurred months/years before or after the privacy concern data collection (Awad and Krishnan, 2006). An implicit assumption here is that individuals' privacy concern remains unchanged between the two separate data collections. Though limited, extant research has found that individuals' privacy concerns could be swayed when they are presented with counter arguments (Baek, 2014). However, current research viewed counter arguments homogeneously and only compared the presence versus. (vs. hereafter) absence of counter arguments. This study seeks to extend the current research by distinguishing between *privacy amplifying arguments* (i.e., counter arguments that seek to increase individuals' privacy concerns) and *privacy diminishing arguments* (i.e., counter arguments that seek to reduce individuals' privacy concerns) to see if they differ in their swaying influence. In addition, we would like to understand what factors may moderate the swaying impact of amplifying vs. diminishing arguments. This study asks the following questions:

> *Research question 1: Do (amplifying vs. diminishing) arguments (similarly or differently) change individuals' privacy concerns?*
>
> *Research question 2: What factors may moderate the above impact and how?*

Understanding the above research questions are of 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 arguments, researchers need to take this into considerations when designing their studies. Practically, understanding how (amplifying vs. diminishing) arguments may change individuals' privacy concerns and the possible moderating factors 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 towards government collecting mobile phone data, individuals, during COVID-19 pandemic, showed greater tolerance after knowing how mobile phone data helps with contact tracing and related issues such as quarantine enforcement; many individuals even voluntarily signed up to use related apps/websites and provide personal data to help with those issues (Fahim, Kim and Hendrix, 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/or regarding how to counteract undesired swaying influences (e.g., what can we do, such as increasing individuals' privacy-related knowledge, to reduce the swaying influence).

The remaining of the paper will be structured as follows. The theoretical basis, awareness-motivation-capability perspective, is introduced first. Then, we present our hypotheses regarding the swaying influence of amplifying vs. diminishing counter arguments on individuals' privacy concerns and moderators for the influence. After that, we discuss data collection and analysis, before presenting our results. Discussion, limitations and future research are provided in the end.

## Literature Review

### *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, Su, and Tsai, 2007). *Awareness* represents an individual's perception of its 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. AMC has been used to examine issues at both the organizational level, e.g., firms' competitive tension (Shi, Connelly, Hoskisson and Ketchen, 2020) and the individual level, e.g., employees' compliance with security policies (e.g., Chen, Chen and Wu, 2018).

The AMC perspective is appropriate for our research on changes in privacy concerns, as it has been successfully applied to understand similar issues such as knowledge adoption (Sussman and Siegal, 2003). As detailed later, 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.

## Hypothesis Development

In this section, we apply the AMC perspective to understand the swaying influence of (amplifying vs. diminishing) counter arguments on individuals' privacy concerns. Specifically, we argue that the presenting of (amplifying or diminishing) counter arguments makes individuals recognize the possible "flaws" in their initial privacy concerns, corresponding to the awareness component of the AMC perspective. In addition, such swaying influence is moderated by the level of sensitivity of the collected information and by individuals' privacy-related knowledge, corresponding to the motivation and to the capability components of the AMC perspective respectively. Figure 1 illustrates our research model.

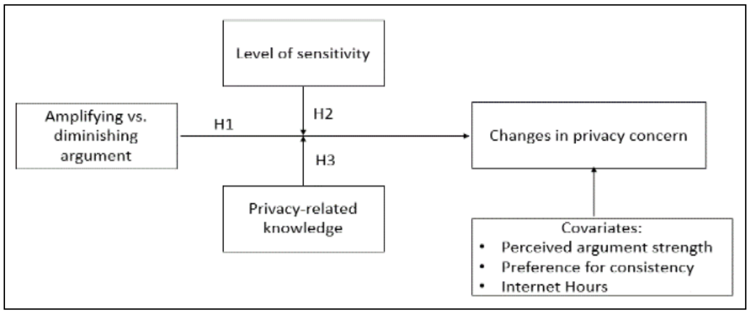
Level of sensitivity
Amplifying vs. diminishing argument
H1
H2
H3
Changes in privacy concern
Privacy-related knowledge
Covariates:
• Perceived argument strength
• Preference for consistency
• Internet Hours

**Figure 1. Research Model**

## Awareness: Amplifying vs. diminishing counter arguments

For individuals to change their opinions, whether about privacy or about other issues, an important prerequisite is to be aware of counter arguments that challenge their current opinions (e.g., Chen 1996). The potential swaying impact of counter arguments has been well examined in the persuasion literature in psychology (e.g., Hass and Linder, 1972; Petty and Cacioppo, 1979; McGuire 1961). Individuals' privacy concerns have been found to be highly superficial and subject to many possible influences such as social expectations (Barth and Jong, 2017; Williams 2017). The possible swaying impact of counter arguments on individuals' privacy concerns, however, has received limited attention in the extant privacy literature. 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 arguments. However, Baek (2014) only examined the presence vs. absence of counter arguments, and it is unclear whether different types of counter arguments—amplifying vs. diminishing arguments—have similar or different swaying impacts.

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

> *H1: Amplifying arguments lead to bigger changes in individuals' privacy concerns than diminishing arguments.*

## Motivation: Level of sensitivity

Level of sensitivity (or information sensitivity) refers to "the potential loss associated with the disclosure of that information" (Mothersbaugh, Foxx, Beatty and Wang, 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, 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 arguments when they do not care much about the issue (e.g., McGuire 1961). We suspect that level of sensitivity may moderate the swaying influence of counter arguments by increasing individuals' concern with the issue and consequently the cognitive efforts they allocate to process those arguments. The higher the level of sensitivity, the more individuals care about the privacy issue (Mothersbaug et al., 2012), the more cognitive efforts they allocate for argument processing (Petty and Cacioppo, 1986; Petty, Cacioppo and Goldman, 1981; Ratneshwar and Chaiken, 1991), and consequently the greater the swaying influences. Our hypothesis can find support in the extant literature. For example, Sussman and Siegal (2003)'s 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 the level of sensitivity. The higher the level of sensitivity, the greater the swaying influence (i.e., bigger changes in privacy concerns).*

### *Capability: Privacy-related knowledge*

Privacy-related knowledge, corresponding to the capability component of the AMC perspective, may also moderate the swaying influence of counter arguments. Research indicates that when individuals are knowledgeable about a topic, their opinions tend to be more stable and less likely to be swayed (e.g., Baek 2014; Converse 1964; Simpson, Siguaw, and Cadogan, 2008; Zaller 1992). For example, e-commerce research found that other consumers' statements (e.g., product/service reviews) and behaviors (e.g., purchase) have a smaller influence on individuals' purchase intention when individuals have higher knowledge and expertise related to the products/services (Cheung, Bo and Liu, 2012). We suspect that the swaying influence of (amplifying or diminishing) arguments is likely to be stronger for those with low privacy-related knowledge. Hence,

> *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*

#### Sample

Respondents were college students enrolled at a public Midwestern university in the US. Data was collected using an online survey, which proceeded as follows: After obtain ing respondents' consent, the survey collected demographic data, history of privacy intrusion, experience with mobile applications and privacy-related knowledge; next, respondents were randomly presented with one of three scenarios (Instagram, Fitbit or WeChat)—those scenarios, as explained later, were chosen for this sample; then, respondents' initial privacy concern and level of sensitivity were measured; after that, respondents were randomly presented with either amplifying or diminishing arguments for the same scenario (Instagram, Fitbit or WeChat); in the end, respondents' privacy concerns were measured again as well as the perceived argument strength of the amplifying or diminishing argument.

215 undergraduate 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 if the survey was 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.

| 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 |
| Internet Hours ((i.e., hours spent using the Internet per day) | 4.861 | 2.662 |
| Privacy intrusion (no prior experience =1, prior experience =2) | 1.51 | 0.503 |

**Table 1. Respondent Demographics**

#### Construct

**Independent variable**. The independent variable is the presenting of amplifying vs. diminishing counter arguments and is manipulated in this study. As described above, respondents, after being first presented with 1 of 3 randomly selected scenario, were subsequently and randomly presented with either amplifying or diminishing arguments for that scenario[1].

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 arguments* talk about the great emphasis that companies (behind health apps like Fitbit) place on protecting health data due to their legal and ethical obligations. The arguments mention companies' heavy investment in data security technologies and experts, mandatory and regular employee training, and the encryption and de-individualization of user data. Even in the incidence of data breach, the de-individualization of user data would make it almost impossible to tell which data belongs to which user. The subsequent *amplifying arguments*, however, first mention that a study of 60 different health apps found that none of them followed best practices for informing user about privacy. Vey 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.

**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, and again after they were presented with either amplifying or diminishing arguments. The *absolute* difference between the two scores reflects changes in individuals' privacy concerns. Measurement items were adapted from Cho et al (2010), i.e., "I am concerned that the information I submit on the Internet could be misused", " When I shop on-line, I am concerned that the credit card information can be stolen while being transferred on the Internet", "I am concerned about submitting information on the Internet because of what others might do with it", and "I am concerned about submitting information on the Internet because it could be used in a way I did not foresee".

**Moderator**. One of the two moderators is privacy-related knowledge, and it was measured by adapting Hargittai and Hsieh (2009). Specifically, respondents were asked to rate their own understandings of spyware, malware, phishing, advanced search, tagging, Wiki, JPG, PDF, Weblog, and Cache.

The other moderator is level of sensitivity, and we handled it in two different ways: we first 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 the level of sensitivity via the three scenarios, i.e., Instagram, Fitbit and WeChat, as discussed below.

Existing information sensitivity research (e.g., Kokolakis 2017; Mothersbaugh et al., 2012) focused on the sensitivity level of different types of information (e.g., contact information, general financial information, and media usage information), and suggested that different types of information trigger varying levels of privacy concerns (Mothersbaugh, Foxx, Beatty, and Wang, 2011). Individuals, for example, are generally more comfortable with disclosing age than with disclosing address or income information. However, websites and mobile applications 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 level of sensitivity of all information collected by different websites and mobile applications. In this study, we picked three mobile applications (i.e., Instagram, Fitbit and WeChat) that likely vary in the level of sensitivity considering their different focuses 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 arguments.

**Control variable**. Control variables include internet hours (i.e., the number of hours individuals spend on Internet per day) and the following two: 1). Preference for consistency, "a dispositional preference for or against consistent responding" (Cialdini, Trost and Newsom, 1995, p. 319), was measured using the following items, i.e., "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", "I want to be described by others as a stable, predictable person", " Admirable people are consistent and predictable", " The appearance of consistency is

[1] Detailed information about the 3 scenarios (i.e., initial description and subsequent amplifying vs. diminishing arguments for each scenario) is available from authors upon request.

an important part of the image I present to the world", "I don't like to appear as if I am inconsistent", "I dislike people who are constantly changing their opinions", "It is important to me that others view me as a stable person", "I make an effort to appear consistent to others", and "I'm uncomfortable holding two beliefs that are inconsistent"; 2). Perceived argument strength was measured by adapting scales from (Zhao, Strasser, Cappella, Lerman and Fishbein, 2011). Specifically, items used were "The above statement is believable", "The above statement is convincing", "The argument helped me feel confident about my knowledge regarding privacy issues", "Overall, how much do you agree or disagree with the statement?", and "Is the above statement regarding privacy concern a strong or weak argument?".

## *Manipulation Check and Construct Reliability*

We first conducted a manipulation check to see whether our amplifying (diminishing) arguments 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 arguments, p=0.09 for diminishing arguments). 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. Cronbach's Alpha values for measured constructs range from 0.777 to 0.864, indicating good reliability.

## *Data Analysis and Results*

Hypotheses were tested using univariate analysis. Data was standardized before being analyzed. We argue that amplifying arguments may lead to a bigger change in privacy concerns as compared to diminishing arguments (H1). Results (left side of Table 2) show that H1 was not supported. We also hypothesize that the swaying influence of amplifying vs. diminishing arguments is moderated by the level of sensitivity (H2) and by privacy-related knowledge (H3). Results (right side of Table 2) show a significant interaction between amplifying vs. diminishing arguments and level of sensitivity.

| **Results for H1** | | **Results for H2-H3** | |
|---|---|---|---|
| Amplifying vs. Diminishing **(H1)** | 0.150 | Amplifying vs. Diminishing | 0.296+ |
| Diminishing argument as the comparison base group | | | |
| Scenario =Instagram | -0.325 | Scenario =Instagram | -0.326+ |
| Scenario=Fitbit | -0.188 | Scenario=Fitbit | -0.226 |
| The WeChat Scenario as the comparison base group | | | |
| Level of sensitivity | 0.156+ | Level of sensitivity | -0.002 |
| Privacy-related knowledge | -0.094 | Privacy-related knowledge | -0.198+ |
| Internet hours | 0.083 | Internet hours | 0.030 |
| Preference for consistency | -0.033 | Preference for consistency | 0.016 |
| Perceived argument strength | -0.080 | Perceived argument strength | -0.092 |
| | | Amplifying vs. diminishing * Level of sensitivity **(H2)** | **0.452**** |
| | | Amplifying vs. diminishing * Privacy-related knowledge **(H3)** | 0.151 |

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

**Table 2. Analysis Results**

The left side of Figure 2 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. In addition, the right side of Figure 2 shows that amplifying arguments had the biggest swaying influence in the Fitbit scenario, which was perceived to have the highest level of sensitivity by respondents, while diminishing arguments had the biggest swaying influence in the WeChat scenario, which was perceived to have the lowest level of sensitivity by respondents. This non-linear swaying influence of amplifying vs. diminishing arguments for privacy concerns once again shows the importance of distinguishing the different types of counter arguments in future research.

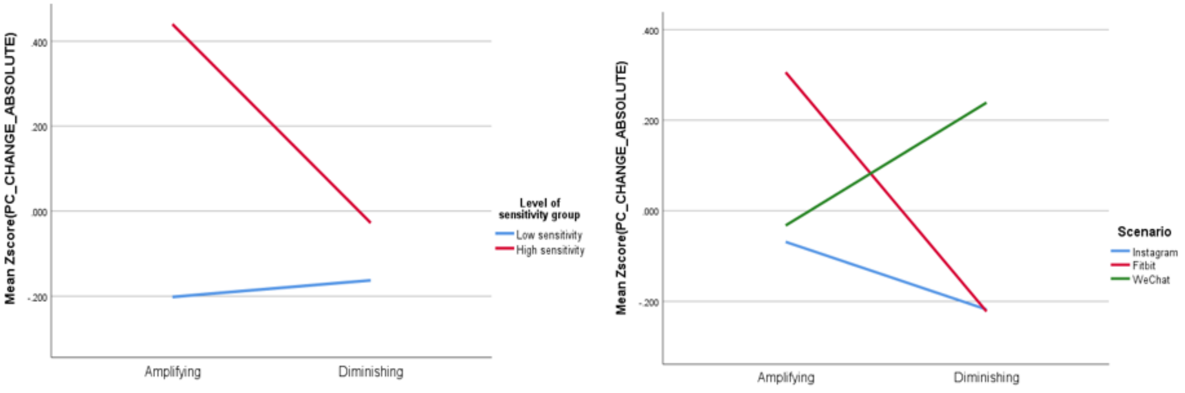

**Figure 2. 2-way Interactions between Amplifying vs. Diminishing Arguments and Level of Sensitivity and between Amplifying vs. Diminishing Arguments and Scenario**

The interaction between amplifying vs. diminishing arguments 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 arguments, privacy -based knowledge and scenario (Figure 3). Figure 3 shows that, for individuals with low privacy knowledge, amplifying arguments 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); diminishing arguments, however, showed the opposite pattern, showing greatest swaying influence in the WeChat scenario (with lowest sensitivity) and the smallest swaying influence in the Fitbit scenario (with lowest sensitivity), similar to that in the Instagram scenario.

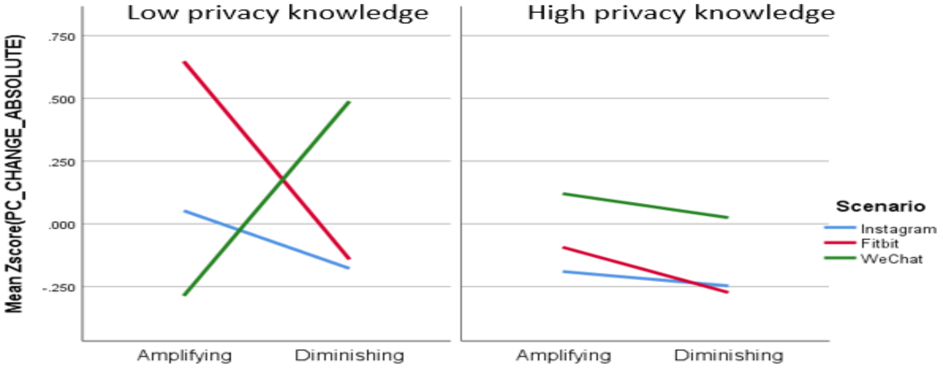

**Figure 3. 3-way Interaction among Amplifying vs. Diminishing Arguments, Privacy-related Knowledge and Scenario**

For individuals with high privacy knowledge, amplifying vs. diminishing arguments showed similar swaying influences, as can be seen from the almost horizontal lines on the right side of Figure 3. 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' higher familiarity with the two apps.

## Discussion

Utilizing the AMC perspective as the underlying theoretical basis, we examined the possible swaying influence of amplifying vs. diminishing counter arguments on individuals' privacy concerns and factors (i.e., level of sensitivity and privacy-related knowledge) moderating the swaying influence. Findings of this study suggest that contrary to our expectation, amplifying arguments did not have a greater swaying influence as compared to diminishing arguments. Instead, the extent of the swaying influence depended on the level of sensitivity and more importantly, the interaction between amplifying vs. diminishing arguments and the level of sensitivity. Specifically, individuals' privacy concerns showed a bigger change when the level of sensitivity is high, especially when individuals were also presented with amplifying arguments. 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 arguments and privacy-related knowledge; instead, we found an almost significant 3-way interaction among amplifying vs. diminishing arguments, privacy-related knowledge and scenario, as discussed later.

The interaction between amplifying vs. diminishing arguments and scenarios (right side of Figure 2) provides interesting insights. First, when presented with either amplifying or diminishing arguments, 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 opinions regarding privacy concerns in Instagram are more set and less likely to be swayed by either amplifying or diminishing arguments. Second and more interestingly, we found that amplifying arguments caused the biggest change in privacy concerns in the Fitbit scenario (with the highest level of sensitivity) while diminishing arguments caused the biggest change in the WeChat scenario (with the lowest level of sensitivity). That is, when the issue or situation is perceived to be high (low) in sensitivity, arguments trying to reduce (increase) individuals' privacy concerns are likely to make a very small difference, while arguments trying to increase (decrease) individuals' privacy concerns are likely to have a big impact. In a word, individuals seem to discount (embrace) privacy counter arguments that are inconsistent (consistent) with their initial assessments, consistent with findings in the psychology literature on cognitive consistency and dissonance (e.g., Festinger, 1957; Gawronski, 2012). Moreover, our examination of the 3-way interaction provides additional insights regarding this, as discussed below.

The left side of Figure 3 suggests that individuals with low privacy-related knowledge are more likely to discount (embrace) privacy arguments that are inconsistent (consistent) with their initial assessments. If the issue or situation is perceived to be high in sensitivity (e.g., Fitbit), privacy concern amplifying arguments caused the biggest changes while diminishing arguments caused the smallest. In contrast, if the issue or situation is perceived to be low in sensitivity (e.g., WeChat), diminishing arguments caused the biggest changes while amplifying arguments caused the smallest change. Comparing the left and the right sides of Figure 3, we can see that although individuals with high privacy knowledge show small changes in privacy concerns in general (i.e., across scenarios and when presented with either amplifying or diminishing arguments), those with low privacy knowledge are only willing to change their privacy concerns when the arguments are consistent with their initial assessments and are reluctant to change when the arguments are inconsistent. That is, individuals with low privacy knowledge also show greater bias when processing privacy related arguments—Just as the old saying goes, individuals with low privacy knowledge tend to "hear what they want to hear" when it comes to privacy related arguments.

## 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 our findings may be different 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, there are other types of applications and devices that are widely used nowadays but raise potential privacy concerns (e.g., smart thermostats and cameras monitoring household activities and schedule, Bluetooth beacons monitoring driving behaviors). Future research testing different scenarios is strongly encouraged.

## Conclusion

This study investigated the swaying influence of amplifying vs. diminishing arguments on individuals' privacy concerns and the moderating impact of level of sensitivity and privacy-related knowledge. Results suggest that the swaying influence of amplifying vs. diminishing arguments depends on the level of sensitivity—the greatest swaying influence happens when individuals are presented with amplifying arguments for a highly sensitive issue or situation. In addition, this study found that individuals with high privacy knowledge show small changes in privacy concerns in general; those with low privacy knowledge, however, are only willing to change, in fact greatly change, their privacy concerns when the arguments are consistent with their initial assessments. If the arguments are inconsistent with their initial assessments, individuals with low privacy knowledge are reluctant to change. In a word, individuals with low privacy knowledge also show greater cognitive bias when processing privacy related arguments.

## REFERENCES

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

Awad, and 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), pp. 13-28.

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

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

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

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017-1041.

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

Chen, M.-J., Su, K.-H., and Tsai, W. 2007. "Competitive Tension: The Awareness-Motivation-Capability Perspective." *Academy of Management Journal* (50: 1), pp. 101–118.

Chen, X., Chen, L., and Wu, D. 2018. "Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective," *Journal of Computer Information Systems* (58:4), pp 312-324.

Cheung, C.M.K., Bo. X., and 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." *45th Hawaii International Conference on System Sciences*. 4-7 Jan. 2012, Maui, HI, USA

Cho, H., Lee, J.-S., and 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), pp. 987–995.

Cialdini, R. B., Trost, M. R., and 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), pp.318–328.

Converse, P. 1964. "The nature of belief systems in mass publics", in *Ideology and discontent,* D. Apter (eds.), New York: Free Press, pp. 206–261

Dinev, Tamara, McConnell, Allen R, & Smith, H Jeff. 2015. "Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box", *Information Systems Research* (26:4), pp. 639-655.

Fahim, K., Kim, M.J., and 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

Festinger, L. 1957. *A theory of cognitive dissonance*, Stanford university press.

Gawronski, B. 2012. "Back to the future of dissonance theory: Cognitive consistency as a core motive," *Social cognition* (30:6), pp 652-668.

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

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

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

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), pp.36–62.

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

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., and Wang, S. 2012. “Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information”, *Journal of Service Research* (15:1), pp. 76–98.

Pavlou, P. 2011. “State of the Information Privacy Literature: Where are We Now and Where Should We Go?” *MIS Quarterly* (35:4), pp. 977-988.

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

Petty, R. E., and 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), pp. 1915–1926.

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

Ratneshwar, S. and 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.

Shi, W., Connelly, B. L., Hoskisson, R. E., and Ketchen, D. J. 2020. "Portfolio Spillover of Institutional Investor Activism: An Awareness–Motivation–Capability Perspective," *Academy of Management Journal* (63:6), pp 1865–1892.

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

Smith, J., Dinev, T., and Xu, H. 2011. “Information Privacy Research: An Interdisciplinary Review.” *MIS Quarterly* (35: 4), pp. 989-1015.

Sussman, S. W., and Siegal, W. S. 2003. “Informational Influence in Organizations: An Integrated Approach to Knowledge Adoption,” *Information Systems Research* (14:1), pp. 47–65

Tversky A, and Kahneman D. 1981. “The framing of decisions and the psychology of choice,” *Science* (211:4481), pp. 453–458.

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

Waldman, Ari Ezra. 2020. “Cognitive biases, dark patterns, and the ‘privacy paradox’,” *Current Opinion in Psychology*, (*31)*, pp. 105-109.

Williams, M., Nurse, J. R. C., and Creese, S. 2017. “Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things,” *2017 15th Annual Conference on Privacy, Security and Trust (PST)*.

Zaller, J. 1992. *The nature and origins of mass opinion*, New York: Cambridge University Press.

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