Who Wants Cookies? Consumer Preferences Towards Privacy Disclosure and Disclosure Benefits: An Exploratory Approach

by

Pakorn Thangchandang
Master of Business Administration program,
Ramkhamhaeng University, Bangkok, Thailand
Tel: +668-524-2555, E-mail: th.pakorn@hotmail.com

and

Snitnuth Niyomsin
Department of Human Resource Management,
Faculty of Business Administration,
Ramkhamhaeng University, Bangkok, Thailand
Tel: +662-310-8547, E-mail: snitnuth.n@rumail.ru.ac.th

IJMBE International Journal of
Management, Business, and Economics

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

Who Wants Cookies? Consumer Preferences Towards Privacy Disclosure and Disclosure Benefits: An Exploratory Approach

by

Pakorn Thangchandang
Master of Business Administration program,
Ramkhamhaeng University, Bangkok, Thailand
Tel: +668-524-2555, E-mail: th.pakorn@hotmail.com

and

Snitnuth Niyomsin
Department of Human Resource Management,
Faculty of Business Administration,
Ramkhamhaeng University, Bangkok, Thailand
Tel: +662-310-8547, E-mail: snitnuth.n@rumail.ru.ac.th

Abstract

This study investigated consumer direct attitudes and explored consumer preferences toward privacy disclosure and disclosure benefits. Taking an exploratory route, conjoint analysis was employed to discover consumer preference patterns and cluster analysis to group consumers based on their preferences. 252 consumers responded to online questionnaires. When asked directly, findings showed participants were very concerned about information disclosure and the risks that came with it. They were somewhat aware of disclosure benefits and moderately intent to disclose their information. When making a tradeoff decision between privacy disclosure and disclosure benefits, the results from conjoint analysis showed that disclosing data to third parties was the most important to participants, followed by benefits from product/service recommendations from third parties. In general, participants seemed to prefer to withhold their information equally to receive personalized product/service suggestions. This equal preference indicated different segments of participants. Findings from cluster analysis showed 6 segments based on their preference – Convenience Lovers, Third-Party Focused, First-Party Cautious, Third-Party Cautious, Personalization Lovers, and First-Party Lovers. Theoretical and practical implications discussed.

Keywords: Privacy concern, Disclosure Benefits, Privacy Calculus, Internet Cookies, Conjoint Analysis

1. Introduction

1.1 Background and Importance of the Problem

More and more, digitalization has been integrated into people’s lives. It transforms the way we work and impacts our daily lives. According to the Thailand Internet User Behavior 2022 report, there were 52.5 million Internet users in Thailand in 2021 accounting for 79.3% of the population (Electronic Transactions Development Agency, 2022).

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

With everything moving online, businesses are competing to give their users better experiences. Personalization plays an important role in enhancing these consumer experiences. To do so, data must be collected. This may cause consumers to lose control over what and how their information may be stored and used. Lee and Cranage (2011) stated that personalization is a process or method of offering services or products that each consumer might want. The goals of personalization are to increase consumer satisfaction and efficiency. To enable web personalization, the use of internet cookies is necessary. The main objective of cookies is to provide consumers with a seamless experience by remembering user preferences and login information, for example. That means information stored by cookies can also be private data that can be used to identify users such as the user's name, email, address, and telephone number (Nguyen & McNally, 2022). Therefore, while cookies can help web services to offer personalized experiences and convenience to consumers, they can sometimes create concerns among consumers about losing control over their own data and how their data is used by businesses.

On June 1st, 2022, Thailand introduced Personal Data Protection Act (PDPA) enforcing web service providers to offer transparency and take accountability in managing and protecting customers' data. This includes obtaining consumers' consent to store their information. Because PDPA is considerably new and involves many details in the implementation, it heavily affects those who offer online services (Prutipinyo, 2022). To help consumers gain control over their data while using web services, businesses are mandated to obtain explicit consent from their users before collecting data. As a result, many web services have popups displaying cookie preferences. Consumers can now choose to accept, reject, or manage some types or combinations of cookies. On one hand, cookies are a vehicle for personalized services that enhance users' online experience. On the other hand, giving away private information in exchange (for improved experience) is not desirable and is viewed as a cost of personalization. In reality, this personalization-privacy paradox may not be so obvious to consumers. They may not be aware of this trade, that is, consumers may not know or understand the trade between personalization and privacy disclosure.

1.2 Research Question

1) What are the consumers' attitudes relating to disclosure intention?

2) Through the use of cookies, what are the consumers' preferences for privacy disclosure and disclosure benefits?

3) How many segments of consumers are there, if any, based on their preferences?

1.3 Research Objective

(1) To understand consumer direct attitudes toward privacy disclosure and disclosure benefits.

(2) To explore consumers' indirect preferences (when presenting with a privacy disclosure - discloser benefits tradeoff).

(3) To discover different consumer segments based on their preferences.

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

2. Literature Review

2.1 Related Concepts and Theories

2.1.1 Web Personalization

With everything moving online, at any given time, a consumer may experience information overload. Too many choices can cause cognitive overstimulation making decision-making much harder. Web personalization can help solve this. The process of personalization, according to Mobasher et al. (2000), involves matching products/services to users. To do so, users' information is needed to create user profiles in order to make personalized recommendations based on their preferences. This information can be given explicitly (such as information a user gives out when setting up an online account) or implicitly (such as browsing history, IP address, or click behavior) (Bozdag, 2013). As a result, personalization can enhance consumers' experience, increase customer satisfaction and loyalty (Ball et al., 2006), and in turn, maximize business opportunities (Ho & Tam, 2005). For consumers, to enjoy personalized experiences, it comes with a price of disclosing their information.

2.1.2 Privacy Calculus Theory

Privacy calculus theory helps explain the privacy paradox (Sun et al., 2022). How individuals make information disclosure decisions depends on the evaluation of the costs of disclosure and the benefits received. This theory assumes that consumers make decisions rationally by comparing the costs and the benefits. If the costs outweigh the benefits, they will be less inclined to disclose. On the other hand, if the benefits outweigh the costs, they will be more inclined.

2.1.2.1 Privacy Concerns

One form of information disclosure costs is privacy concerns. Its relationship with information disclosure has also been much studied in the e-commerce context (Yeh et al., 2018). When people are concerned about the loss of their information or that their privacy may be at risk, they are less willing to disclose information. Wang et al. (2020) found a negative effect of privacy concerns on disclosure intention in the social media sphere. And in the public health domain, privacy concerns was one of the predictors that had a negative influence on willingness to disclose personal information to COVID-19 tracking apps (Fernandes & Costa, 2023).

2.1.2.2 Perceived Privacy Risks

Perceived privacy risks are considered one of the costs of information disclosure (Wang et al. 2022). Harms caused by data leaking are frequently shown in the media. For example, The Bangkok Post reported in 2022 that, in Thailand, more than half of phishing attempts were finance-related (Leesa-Nguansuk, 2022). The effects of perceived risks on disclosure intention have been studied many times (Wang et al., 2022) and generally showed negative effects (Wang et al., 2016; Duan & Deng, 2021).

2.1.2.3 Perceived Benefits

On the other end of the spectrum in privacy calculus theory, there are information disclosure benefits. Perceived benefits serve as one of the disclosure intention predictors (Wang et al., 2022). If the perceived values gained from disclosing information outweigh the costs, people will be more

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

willing to disclose their information. Again, a positive relationship between perceived benefit and disclosure intention was found in most studies in various domains. In the public health domain, disclosure benefits showed a positive impact on willingness to disclose information (Fernandes & Costa, 2023) and adopt contact tracing apps during COVID-19 (Duan & Deng, 2021). In the e-commerce domain, Al-Jabri et al. (2020) found both the perceived benefits (personalization and convenience) influenced willingness to disclose information, and the same findings found by Wang et al. (2016) for mobile applications.

The privacy calculus theory assumes people take a cognitive process in evaluating their choices – i.e., the costs and the benefits of information disclosure. This process also assumes that, first, people are aware that there are costs and benefits associated with privacy disclosure, and second, they recognize the mechanic behind it, that is, there is a tradeoff between the costs and the benefits of information disclosure. These assumptions might not always be the case. A study by Stevenson and Pasek (2015) found that people who had privacy concerns (costs of disclosure) still wanted personalized services (benefits of disclosure). People might not know the relationship between information disclosure and personalization. In other words, they don't know that their personal information makes it possible for personalized services.

RQ1: What are the consumers' attitudes relating to disclosure intention?

2.1.3 Internet Cookies

One of the tools web service providers use to store and track users' information, esp. implicit information, is cookies. Internet cookies are small text files that are stored in users' computers by the browser to identify the users to the network. When visiting websites, cookies will record users' information and activities. So, when users revisit the same website, cookies will identify the users again. Websites will, then, bring back users' information and activity history. This makes it more convenient for the user to continue using the website seamlessly. According to Gourley and Totty (2002), cookies were first developed by Netscape. They explained that in the beginning, there were two types of cookies: session cookies and persistent cookies. Session cookies were temporary and would expire when users closed their browsers. On the other hand, persistent cookies were stored and retained in the computer even after the browsers were closed or the computers were restarted. Persistent cookies were usually used to store the settings or login information of frequently visited websites. The only difference between the session and persistent cookies was the expiration. Later, according to Dubrawsky and Faircloth (2009), the main types of cookies are session, persistent, and tracking cookies.

According to Cooper et al.'s (2023) review, cookies were first designed for websites to provide a better experience to their return users. It was not until later that cookies were used for marketing purposes. Tracking cookies, that allow external parties to access users' information and activities for their marketing purposes, are the most commonly used tool to collect consumer data. Data drawn out by external parties (third parties) or simply sharing user information with them can be considered unethical practices (Gurau et al., 2003) and create privacy risks (Tomy & Pardede, 2016). With PDPA in place, explicit consent about privacy information collection is required. Web service users are now asked to accept, reject, or manage cookies – i.e., how their data are managed.

2.1.4 An Issue with Privacy Calculus Theory

Much research follows the privacy calculus theory to explain the privacy paradox. Most findings were aligned with the theory, showing a negative relationship between the disclosure costs

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

and disclosure intention, and a positive relationship between benefits and disclosure intention. But one issue can't go without notice. As raised by Sun et al. (2022), one of their issues is in the decision-making process. They claimed that people will make a tradeoff decision (between disclosure costs and benefits) rather than each side independently (assume high costs-low benefits and low costs-high benefits). While most studies tested the effects of disclosure costs and benefits on disclosure intention independently, they proposed interdependent effects in their study. They found that when benefits and risks are high people will be more inclined to disclose their information if benefits and risks are justified. In the same situation, if not justified, they will be less inclined. And if the benefits are low, they will be less inclined to disclose regardless of privacy risks.

In this research, rather than focusing on testing effects among variables, we will take an exploratory route to explore people's preferences.

RQ2: Through the use of cookies, what are the consumers' preferences for privacy disclosure and disclosure benefits?

RQ3: How many segments of consumers are there, if any, based on their preferences?

3. Research Methodology

This research employed a quantitative approach using an online questionnaire to collect data. Because the research aimed to explore consumers' preference for privacy disclosure-discloser benefits, conjoint analysis was employed. In the real world, when using web services, consumers are asked to accept, reject, or manage cookies in settings – with different kinds of cookies presented in the settings. From the literature, it is possible that consumers might not want to disclose their information while wanting a personalized service. This is because they might not know about the trade between disclosing personal information and receiving personalized services. For this reason, conjoint analysis was employed. In the conjoint tasks, because choices are presented in full profile, this method also allows this study to measure indirect preference between privacy disclosure and disclosure benefits. Traditional conjoint analysis was chosen because it yielded results at the individual level. Therefore, it can measure the preference of just 1 participant (Orme, 2010). But in general, the sample size is between 150 to 1,200 participants (Orme, 2010). However, Hair et al. (2010) suggested an appropriate sample size of 200.

3.1 Research Design

3.1.1 Establishing Conjoint Attributes and Levels

To determine appropriate attributes and levels, three experts were interviewed. The three experts consisted of a web developer, an application developer, and an online advertisement consultant. The objectives of the interview were to determine how web services gather information from their users and what benefits users can experience. The results from the interview were, then, used to finalize attributes and levels, as shown below.

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

Table 1 Summary of Attributes and Levels

Attribute	Level
Information collected by the present web service (first party)	Yes No
Information collected by other web services (third party)	Yes No
Website remember your last session information	Yes No
Products/services suggestion by the present web service (first party)	Random suggestion Personalized suggestion
Products/services suggestions by other web services (third party)	Random suggestion Personalized suggestion No suggestion

The attributes and levels in Table 1 yielded a total of 48 combinations. Rating 48 combinations could cause exhaustion. A fractional factorial design was employed, yielding 8 combinations with 4 holdouts to test the reliability of the measurement – a total of 12 combinations were used.

3.2 Population, Sample and Data Collection

Participants were those who had bought products or used services from online web services. Convenience and voluntary response sampling methods were employed. The link to the online questionnaire was distributed through convenience sampling. To ensure the diversity of the participants, the survey link was also posted on social networks and various social media. In total, four hundred and fifteen responses were returned. Of those, 252 responses were completed (and usable) and included in this research.

3.3 Research Instruments

This research employed an online questionnaire for data collection. The questionnaire consisted of:

First is the conjoint part to measure indirect preference. A hypothetical situation "assume you were to buy a product/service online, there were 12 online stores offering the same product/service with different cookie settings" was used to introduce this task to the participants. Participants were, then, asked to rate their willingness to buy the product/service from each store from 0-10 (suggested by Hair et al. 2010), with 0 being "absolutely will not buy from this store" and 10 being "absolutely will buy from this online store." In this survey, we started with the conjoint tasks, which aimed to answer research 2. This is because rating various full-profile situations requires more effort and conjoint tasks are the heart of this study. Hence, conjoint tasks were put at the beginning of the questionnaire to prevent raters' fatigue.

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

The second part of the survey aims to measure direct attitudes toward privacy disclosure and disclosure benefits. This study followed Phonthanukitithaworn and Sellitto (2022) for the "general privacy concerns" variable, Dinev et al. (2013) for "perceived privacy risks" and "perceived benefits of information disclosure", Malhotra et al. (2004) for "general institution trust", and Zhu et al. (2022) for the "privacy disclosure intention." All were reflective variables and a five-point Likert-typed scale was used to measure the variables, with 1 being "strongly disagree" and 5 being "strongly agree."

The last part of the questionnaire consisted of demographic information questions.

Once the questionnaire design was completed, pretesting was performed with five consumers who have used web services. There were some questions in the first two parts of the questionnaire. The questionnaire was, then, revised and pretested two more times with different sets of consumers. After the pretesting was done, pilot testing was performed with another 50 consumers who have used web services. Cronbach's alpha of variables measuring direct attitudes in research question 1 (the second part of the questionnaire) ranged from .825 to .914.

3.4 Statistics Used for Data Analysis

Descriptive and correlation analyses were employed to measure direct attitudes toward privacy disclosure and disclosure benefits in research question 1. For research question 2, conjoint analysis was employed to measure consumers' preferences. For research question 3, first, hierarchical cluster analysis was employed to group consumers based on their preferences, then conjoint analysis was performed again on each cluster to gain further insight.

4. Data Analysis and Findings

4.1 Introduction

Of the 252 participants, 159 were females and 93 were males, accounting for 63.1 and 36.9 percent accordingly. Fifty-six percent were Generation Y (age ranging from 27 – 42 years old) and 65.5 percent were single. Lastly, 71 percent of the participants held a bachelor's degree and 46 percent are working in the private sector.

4.2 Data Analysis of the Qualitative Data

4.2.1 RQ1: What are the consumers' attitudes relating to disclosure intention?

Table 2 Descriptive Analysis (n = 252)

Attitudes Relating to Disclosure Intention	M	S.D.	Level
General privacy concerns (cost)	4.59	0.59	very high
Perceived risks of information disclosure (cost)	4.31	0.73	very high
Perceived benefits of information disclosure	3.23	1.12	moderate
Intention to disclose	2.83	1.09	moderate

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

Results from Table 2 show that, when asked directly, participants were very concerned about their privacy (M = 4.59, SD = 0.59). They also expressed a very high level of perceived risks that came with disclosing their information (M = 4.31, SD = 0.73). On the other hand, they were moderately aware of the benefits that came with disclosing their information (M = 3.23, SD = 1.12) and reported moderate intention to disclose their information (M = 2.83, SD = 1.09).

Table 3 Correlation Analysis (n = 252)

	(1)	(2)	(3)	(4)
(1) General privacy concerns (cost)	1			
(2) Perceived risks of information disclosure (cost)	.549**	1		
(3) Perceived benefits of information disclosure	-.210**	-.115	1	
(4) Intention to disclose	-.310**	-.147*	.488**	1

* p < 0.05, ** p < 0.01, *** p < 0.001

Findings from Table 3 indicated negative correlations between intention to disclose and both general privacy concerns (r = -.310, p < .001) and perceived risks of information disclosure (r = -.147, p < .005). The more participants are concerned about their privacy, the less likely they will disclose their information. On the other hand, results showed positive correlations between intention to disclose and both perceived benefits (r = .488, p < .005). This means the more the participants perceived disclosure benefits (e.g., personalization), the more likely they will disclose their information. Perceived benefit was also negatively correlated with general privacy concerns (r = -.210, p < .001). Participants who realized the benefits of disclosing information were less concerned about their privacy.

4.2.2 RQ2: Through the use of cookies, what are the consumers' preferences for privacy disclosure and disclosure benefits?

Table 4 Part-Worth Estimations

Attribute	Level	P-W	S.E.
Information collected by the present web service (first party)	Yes	-.244	0.02
	No	**.244**	0.02
Information collected by other web services (third parties)	Yes	-.928	0.02
	No	**.928**	0.02
Website remember your last session information (convenience)	Yes	**.268**	0.02
	No	-.268	0.02
Product/service suggestions by the present web service (first party)	Random suggestion	-.369	0.02
	Personalized suggestion	**.369**	0.02
Product/service suggestions by other web services (third parties)	Random suggestion	-.073	0.03
	Personalized suggestion	**.090**	0.03

	No suggestion	-.017	0.03

Findings from Table 4 show that, ideally, participants preferred to withhold their information (part-worth utility of .244 and .928), yet wanted to receive personalized benefits i.e., product/service suggestions from first and third parties (part-worth utility of .369 and .090). They also prefer to receive convenience from the website remembering last session activities (part-worth utility of .268) – such as not having to fill in the same information again the next time they log in.

Table 5 Importance Values (n = 252)

Attribute	Importance Values
Information collected by the present web service (first party)	18.16
Information collected by other web services (third parties)	26.66
Website remember your last session information (convenience)	14.77
Product/service suggestions by the present web service (first party)	15.16
Product/service suggestions by other web services (third parties)	25.26

Findings from Table 5 indicate the importance of third parties. Participants focused more on third parties than the first party in both privacy disclosure (importance values of 26.66 versus 18.16) and disclosure benefits (importance values of 25.26 versus 15.16). In other words, they were more concerned about other web services (third parties) collecting their data than the first party. They also focused more on personalized product/service suggestions from other web services than the present web service.

Results from both Table 4 and 5 indicated that, when comparing a tradeoff preference, participants, on average at the aggregated level, still preferred to withhold their information equally to receive personalized product/service suggestions (importance values of 18.16 versus 15.16 for first party and 26.66 versus 25.26 for third parties). These results revealed there may be different segments of consumers based on their preferences. This is because traditional conjoint analysis provides estimations at the individual level, so the overall results in Table 4 and Table 5 were just an average of all the participants' estimations.

4.2.3 RQ3: How many segments of consumers are there, if any, based on their preferences?

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

Table 6 Segments from Cluster Analysis

Cluster and Mean Value						
Segment	**1**	**2**	**3**	**4**	**5**	**6**
n = 252	52	84	23	28	59	6
(100%)	20.60%	33.30%	9.10%	11.10%	23.40%	2.40%
Information collected by the present web service (first party)	18.48	17.63	44.34	12.82	13.02	7.60
Information collected by other web services (third parties)	17.45	33.25	12.83	63.53	11.43	21.43
Website remember your last session information (convenience)	30.58	10.20	6.90	6.67	15.31	20.68
Product/service suggestions by the present web service (first party)	9.00	12.89	10.91	2.41	29.18	43.37
Product/service suggestions by other web services (third parties)	24.51	26.04	25.06	14.61	30.09	6.97

Results from cluster analysis in Table 6 showed six segments. By clustering the important values (results from conjoint analysis), six segments based on their preferences were revealed. To gain further insight into each segment's preference, conjoint analyses were performed again for part-worth utilities on each cluster (since all 6 clusters are based on important values, not part-worth utilities). Table 7 showed the detailed preferences of each cluster.

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

Table 7 Summary of Part-Worth Utilities for Each Cluster

Attribute	Level	Cluster 1		Cluster 2		Cluster 3		Cluster 4		Cluster 5		Cluster 6	
		P-W	S.E.	P-W	S.E.	P-W	S.E.	P-W	S.E.	P-W	S.E.	P-W	S.E.
Information collected by the present web service (first party)	Yes	-.079	.010	-.411	.046	-.641	.146	-.379	.088	**.028***	.072	**.167***	.147
	No	.079	.010	.411	.046	.641	.146	.379	.088	-.028	.072	-.167	.147
Information collected by other web services (third parties)	Yes	-.531	.010	-1.417	.046	-.370	.146	-2.281	.088	-.197	.072	-.524	.147
	No	.531	.010	1.417	.046	.370	.146	2.281	.088	.197	.072	.542	.147
Website remember your last session information (convenience)	Yes	.531	.010	.182	.046	.152	.146	.058	.088	.328	.072	.042	.147
	No	-.531	.010	-.182	.046	-.152	.146	-.058	.088	-.328	.072	-.042	.147
Product/service suggestions by the present web service (first party)	Random suggestion	-.113	.010	-.348	.046	-.185	.146	-.122	.088	-.778	.072	-.750	.147
	Personalized suggestion	.113	.010	.348	.046	.185	.146	.122	.088	.778	.072	.750	.147
Product/service suggestions by other web services (third parties)	Random suggestion	-.157	.014	**.091***	.062	.043	.195	.030	.118	-.331	.096	-.056	.230
	Personalized suggestion	.232	.16	.008	.072	-.337	.228	.119	.138	.229	.112	.153	.230
	No suggestion	-.075	.16	-.099	.072	**.293***	.228	-.149	.138	.102	.112	-.097	.155

Note: *Highest part-worth utility (most preferred) that differs from the results from aggregated level (in Table 4)

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

To understand each cluster clearly and describe them in a meaningful way, descriptions of each cluster were based on results from Table 6 and Table 7 combined.

Cluster 1: Convenience Lovers, accounted for 20.60%. Compared to other clusters, convenience was really important to them. They wanted websites to remember their previous activities, so they could continue easily when revisited. In addition, they also wanted personalized recommendations from third parties.

Cluster 2: Third-Party Focused, accounted for 33.30%. Participants in this cluster paid the most attention to both costs (privacy disclosure to third parties) and benefits (random suggestions offered by third parties). Preferences of people belonging to this cluster reflected the findings from research question 2. Note that random suggestions are benefits that don't require privacy disclosure i.e., a tradeoff.

Cluster 3: First-Party Cautious, accounted for 9.10%. Compared to other clusters, they were really concerned about information collected by the first party. They also didn't care much about the benefits offered by the first party. In addition, they very much preferred no suggestions (benefits) from third parties.

Cluster 4: Third-Party Cautious, accounted for 11.10%. Participants in this cluster seemed to be concerned about information collected by third parties. They simply didn't want to disclose their information to third parties. On the other hand, they wanted personalized benefits from third parties. But it was obvious that privacy disclosure substantially outweighed disclosure benefits (importance values of 63.53 vs. 14.61).

Cluster 5: Personalization Lovers, accounted for 23.40%. Participants in this cluster simply just wanted personalized services from both first and third parties. They also wanted to receive convenience when using the website and prefer to disclose their information to first party.

Cluster 6: First-Party Lovers, accounted for only 2.40%. This small group of participants wanted the benefits offered by first party. They also had no problem revealing their information to first party. On the other hand, they neither wanted to disclose information nor received personalized benefits from third parties.

5. Conclusion, Discussion, and Recommendation

5.1 Conclusion

5.1.1 RQ 1:

When asked directly, participants were concerned about their privacy and were aware that there may be risks associated with information disclosure. This is not surprising. However, when asked about the perceived benefits, participants were only moderately aware. This could be explained by limited knowledge, or lack thereof for some, of how the algorithm works. Because the algorithm is invisible, people might not realize they are getting a personalized service (benefits) while using websites (Koene et al., 2015).

In general, disclosure intention was positively correlated with perceived benefits and negatively correlated with perceived risks and concerns. Perceived benefits were more correlated

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

with disclosure intention than disclosure concern and perceived risks. This is in line with findings from research question 3 (discussed later) that most consumers focus more on the benefits than the costs of disclosing.

The result from research question 1 showed an inconsistency between perceived benefits and disclosure costs (concerns and risks). While perceived benefits were weakly and negatively correlated with general disclosure concerns (suggesting a weak tradeoff), they had no significant relationship with perceived risks. Rating each variable independently could be the cause of this inconsistency or participants might not be aware of the relationship between disclosure costs and benefits. Findings from research questions 2 and 3 could help explain.

For the inconsistency between both disclosure costs (concerns and risks) and perceived benefits, on the surface, aggregated results from conjoint analysis (Table 4 and Table 5) seemed to yield the same trends. That is, overall, it seemed people didn't want to disclose the information (cost) but wanted personalized benefits. The importance of privacy disclosure is almost equal to the importance of disclosure benefits. But when cluster analysis was performed on the importance values of individuals, six different segments with unique preference patterns were revealed. This suggests consumer preferences are more complex than just simple ratings. Some people focused on benefits, some on cost, and most were in between with different proportions of wanting benefits and not wanting to disclose information. This is simply not a zero-sum game. And the presence of the "to whom" they disclose information or "from whom" they receive benefits makes decision-making more complicated.

Overall, full-profile displays in the conjoint tasks offer some elements of tradeoff and yield a more realistic picture to raters. Therefore, the outcomes from conjoint analysis are much different than those from a straight-forward rating.

5.1.2 RQ 2:

The part-worth utilities showed that, ideally, people want benefits but don't want to give out their information. As Sun et al. (2022) mentioned, the situation might not have to be with obvious net values (high costs-low benefits and low costs-high benefits). And the decision-making process may be more complex by adding to and from whom participants disclose information or receive the benefits – that is, first and third parties.

When looking at the importance values, there are two issues that need to be discussed:

First, findings showed a much stronger focus on third parties in both costs (privacy disclosure) and benefits (personalization) than on first party. The strong focus on third-party costs might not be so surprising. This may be because (1) people intend to visit the first-party website, not other businesses, and (2) people might not know or recognize who the third parties are. These two reasons can put people on the defensive mode and take extra caution in exposing their information to third parties. For the strong focus on third-party benefits, an increase in consumers' online activities nowadays may be an explanation. Convenience and personalized recommendations can save time and reduce cognitive overstimulation.

Second, when taking a closer look at first-party and third-party attributes, results showed the same trends – i.e., privacy disclosure to the first party is almost equally important to disclosure benefits by the first party. Again, costs and benefits are equally important. People don't want to give out information but still want personalized benefits. And the same results go to third parties also.

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

personalization paradox. While privacy-personalization is a tradeoff process in nature, not all benefits require privacy disclosure. For example, a randomized product suggestion can be considered a benefit without requiring privacy disclosure. (Randomized suggestions allow an increase in suggestion diversity, while personalization can be overspecialized and reduce suggestion diversity.) Conjoint method helps to explore people's preferences and close the gap where researchers had to make assumptions about whether the tradeoff is known or not known to participants. This can be done because, in the conjoint method, various situations are displayed in such a way (full profile concept card) that forces participants to be aware of all the situations and rate their preferences accordingly. We, therefore, eliminated the assumption issue and were able to explore people's preferences giving them full information (allowing interdependence between costs and benefits).

Second, the to- and from- "whom" aspects should be considered when taking on the privacy calculus theory in the online domain. Consumer preferences are different toward disclosing their information to first party or third parties. The benefits they receive from first party and third parties are also different. When there is more than one party involved, the decision-making is more complex. Therefore, in the domain where more than one party is involved, this to- and from- "whom" issue should be addressed.

5.2.2 Practical Implications

Drawing from some parts of the research findings, we can form some suggestions for businesses. From the preference profiles of the three biggest segments (Third-Party Focused, Personalization Lovers, and Convenience Lovers, accordingly), which accounted for over 70% of participants, benefits are the most important. And from the biggest segment (Third-Party Focused), information collection from third parties is very important and undesirable.

First is bringing the benefits to the top. If businesses want to collect users' information, when asking for consent, make sure users know the benefits they will get before anything else. The first impression should be a positive thing they care about the most.

Second, what they are most concerned about – i.e., information collection by third parties – should be the last. Permission for third parties to collect information should be last in the consent form. Make sure people are aware and understand all the benefits of disclosing their information before asking to collect their information.

By showcasing the benefits at the top with a convincing explanation of disclosure benefits and costs, people may feel that the benefits they receive justify the costs. It also promotes transparency. This, in turn, may increase the chance for information collection.

5.3 Recommendation

Limitations and Directions of Future Research

This research has some limitations. The data collection in this research was through an online questionnaire. There are some limitations when distributing questionnaires online. Self-selection bias could occur when using voluntary response samples. People who opted to participate were self-selected and might have certain attitudes or experiences that differed from those who opted not to participate.

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

Future research in the realm of privacy calculus theory could include the to- and from-"whom" condition in their model to gain insight into consumers' attitudes in a more realistic way. Distinguishing costs and benefits from first and third parties are also a part of decision-making.

Taking the same exploratory route in different domains is also worth mentioning. People's attitudes are probably much different when testing in, for example, healthcare, social networks, or online content domains. When people get telehealth services, they may respond to the disclosure costs, benefits, and intentions differently than when they serve the Internet.

References

Al-Jabri, I. M., Eid, M. I., & Abed, A. (2020). The willingness to disclose personal information: Trade-off between privacy concerns and benefits. *Information & Computer Security*, 28(2), 161-181. Emerald Publishing Limited. ISSN 2056-4961. doi:10.1108/ICS-01-2018-0012.

Ball, D., Coelho, P. S., & Vilares, M. J. (2006). Service personalization and loyalty. *Journal of Services Marketing*, 20(6), 391–403. Emerald Group Publishing Limited. ISSN 0887-6045. doi:10.1108/08876040610691284.

Bozdag, E. (2013). Bias in algorithmic filtering and personalization. *Ethics Inf Technol*, 15, 209-227. DOI: 10.1007/s10676-013-9321-6.

Cooper, D. A., Yalcin, T., Nistor, C., Macrini, M., & Pehlivan, E. (2023). Privacy considerations for online advertising: A stakeholder's perspective to programmatic advertising. *Journal of Consumer Marketing*, 40(2), 235-247. Emerald Publishing Limited. ISSN 0736-3761. doi:10.1108/JCM-04-2021-4577.

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

Duan, S. X., & Deng, H. (2022). Exploring privacy paradox in contact tracing apps adoption. *Internet Research*, 32(5), 1725-1750. Emerald Publishing Limited. ISSN 1066-2243. doi:10.1108/INTR-03-2021-0160.

Dubrawsky, I., & Faircloth, J. (2009). *Eleventh Hour Security+: Exam SY0-201 Study Guide* (1st ed.). Burlington, MA: Syngress.

Electronic Transactions Development Agency (ETDA). (2022). *Thailand Internet User Behavior 2022*. Retrieved from https://www.etda.or.th/getattachment/78750426-4a58-4c36-85d3-d1c11c3db1f3/IUB-65-Final.pdf.aspx.

Fernandes, T., & Costa, M. (2023). Privacy concerns with COVID-19 tracking apps: A privacy calculus approach. *Journal of Consumer Marketing*, 40(2), 181-192. Emerald Publishing Limited. ISSN 0736-3761. doi:10.1108/JCM-03-2021-4510.

Gourley, D., & Totty, B. (2002). *HTTP: The Definitive Guide. Sebastopol*, CA: O'Reilly Media.

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

Gurau, C., Ranchhod, A., & Gauzente, C. (2023). "To legislate or not to legislate": A comparative exploratory study of privacy/personalization factors affecting French, UK, and US websites. *Journal of Consumer Marketing*, 20(7), 652-644. MCB UP Limited. ISSN 0736-3761. doi:10.1108/07363760310506184.

Hair, F. J., Black, C. W., Babin,J. B., & Anderson, E. R.(2010). *Multivariate Data Analysis: A global perspective* (7th ed.).New Jersey: Pearson Education, Inc.

Ho, S. Y., & Tam, K. Y. (2005). An empirical examination of the effects of Web personalization at different stages of decision making. *International Journal of Human-Computer Interaction*, 19(1), 95-112.

Koene, A., Perez, E. J., Carter, J. C., Statache, R., Adolphs, S., O'Malley, C., Rodden, T., & McAuley, D. (2015). Privacy concerns arising from Internet service personalization filters. *Durham Research Online*, 45 (3), 167-171. DOI:10.1145/2874239.2874263.

Lee, C. H., & Cranage, D. A. (2011). Personalisation Privacy Paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites. *Tourism Management*, 32(5), 987-994.

Leesa-Nguansuk, S. (2022, July 8). *Thailand leads in e-shop phishing. Bangkok Post, Business section*. Retrieved from https://www.bangkokpost.com/business/2341932/thailand-leads-in-e-shop-phishing.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4), 336-355. ISSN 1047-7047/EISSN 1526-5536/04/1504/0336.

Mobasher, B., Cooley, R., & Srivastava, J. (2000). Automatic personalization based on Web usage mining. *Communications of the ACM*, 43(8), 142-151.

Nguyen, S. J., & McNally, C. (2022, November 3). *What Are Internet Cookies and How Are They Used?*. AllAboutCookies.org. Retrieved from https://allaboutcookies.org/what-is-a-cookie.

Orme, K. B. (2010). *Getting Started with Conjoint Analysis: Strategies for Product Design and Pricing Research*. (2nd ed.). United States of America: Research Publishers LLC.

Phonthanukitithaworn, C., & Sellitto, C. (2022). A Willingness to Disclose Personal Information for Monetary Reward: A Study of Fitness Tracker Users in Thailand. *SAGE Open*, April-June, 1–15. https://doi.org/10.1177/21582440221097399.

Prutipinyo, C. (2022). PDPA: Personal Data Protection Act, 2019. *Public Health Policy & Laws Journal*, 8(1), 203-214.

Stevenson, D., & Pasek, J. (2015). Privacy Concern, Trust, and Desire for Content Personalization. *Information and Internet Policy Paper*. DOI: 10.2139/ssrn.2587541.

Received: 9 July 2023 / Revised: 23 August 2023 / Accepted: 31 August 2023
@ Sripatum University Press 2023

Sun, Y., Zhang, F., & Feng, Y. (2022). Do individuals disclose or withhold information following the same logic: a configurational perspective of information disclosure in social media. *Aslib Journal of Information Management*, 74(4), 710-726. Emerald Publishing Limited. ISSN 2050-3806. doi:10.1108/AJIM-06-2021-0180.

Tomy, S., & Pardede, E. (2016). Controlling privacy disclosure of third-party applications in online social networks. *International Journal of Web Information Systems*, 12(2), 215-241. Emerald Group Publishing Limited. ISSN 1744-0084. doi:10.1108/IJWIS-12-2015-0045.

Wang, L., Hu, H.-H., Yan, J., & Mei, M. Q. (2020). Privacy calculus or heuristic cues? The dual process of privacy decision making on Chinese social media. *Journal of Enterprise Information Management*, 33(2), 353-380. Emerald Publishing Limited. ISSN 1741-0398. doi:10.1108/JEIM-05-2019-0121.

Wang, N., Zhao, Y., Zhou, R., & Li, Y. (2022). Factors influencing users' online information disclosure intention and the moderating effect of cultural background and platform type. *Aslib Journal of Information Management*, Volume(Issue), Page range. Emerald Publishing Limited. ISSN 2050-3806. doi:10.1108/AJIM-04-2022-0218.

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, 36(4), 531-542. https://doi.org/10.1016/j.ijinfomgt.2016.03.003.

Yeh, C.-H., Wang, Y.-S., Lin, S.-J., Tseng, T. H., Lin, H.-H., Shih, Y.-W., & Lai, Y.-H. (2018). What drives internet users' willingness to provide personal information? *Online Information Review*, 42(6), 923-939. Emerald Publishing Limited. ISSN 1468-4527. doi:10.1108/OIR-09-2016-0264.

Zhu, X., Cao, Q., & Liu, C. (2022). Mechanism of Platform Interaction on Social Media Users' Intention to Disclose Privacy: A Case Study of Tiktok APP. *Information*, 13, 461. https://doi.org/10.3390/info13100461.