COMMUNICATION AND MEDIA IN ASIA PACIFIC (CMAP)
2025, VOL. 8, NO.2, 97-114.
http://doi.org/10.14456/cmap.2025.8

Willingness to Disclose Personal Data for Enhanced Customer Experience through Marketing Technology and Online Data Privacy Personality

Rungpailin Songja[a]*, Patchanee Cheyjunya[a]

[a]National Institute of Development Administration, Thailand

ABSTRACT

As businesses increasingly leverage data collection and marketing technologies to enhance customer experiences (CX), concerns regarding privacy and the protection of personal data remain significant. This study investigates the willingness of Thai consumers to disclose personal information in exchange for improved customer experiences, with a focus on variations across online data privacy personality types. Employing a quantitative approach, data were collected through an online questionnaire administered to 420 Thai consumers aged 18-59 years. Using descriptive statistics, factor analysis, and cluster analysis, the findings reveal that most consumers are willing to share personal (e.g., lifestyle, occupation, acquaintances) and medical information, particularly during the "Ask" phase of the 5A's Customer Path, which involves interactions through robotics, natural language processing (NLP), and sensor technologies. Thai consumers were segmented into four privacy personality clusters: (1) Privacy Controllers, (2) Privacy Savvies, (3) Privacy Challengers, and (4) Privacy Unaware. These insights can inform the development of communication strategies that encourage responsible data sharing and support the effective use of marketing technologies to deliver personalized experiences tailored to each consumer group.

Article Info
Received November 27, 2024
Revised August 21, 2025
Accepted September 2, 2025

Keywords: Willingness to disclose, Personal data, Customer experience, Marketing technology, Data privacy, Thailand

Introduction

In today's digital era, communication increasingly relies on advanced technologies, such as computers, smartphones, and other devices. Data play a critical role in this landscape, as digital platforms, particularly social media, often have access to more intimate information than an individual's family or close friends, sometimes understanding users' preferences better than the users themselves. This vast access to data raises concerns about personal data privacy, particularly regarding the collection and use of data without individuals' full awareness or consent. As a result, data has emerged as a strategic asset for innovation and business development (Wuttidittachotti et al., 2021).

Within the framework of Marketing 5.0, the use of big data and next-generation technologies (e.g., artificial intelligence, chatbots, and robotics)

CONTACT

Rungpailin Songja (B.A., Silpakorn University, Thailand) is a graduate student, Master's Program in Communication Management (Data Analytics), National Institute of Development Administration, Thailand.

Patchanee Cheyjunya (M.A., Chulalongkorn University, Thailand) is Emeritus Professor, Graduate School of Communication Arts and Management Innovation, National Institute of Development Administration, Thailand.

***Corresponding author's email:** rungpailin.sj@gmail.com

enables businesses to deliver personalized products and services aligned with specific customer needs. Marketers are now expected to engage consumers throughout the entire customer journey from awareness to advocacy by using data-driven marketing technologies (Kotler et al., 2021). However, this technological advancement intensifies the debate around digital ethics and privacy.

According to Cisco (2020), 60% of global consumers are concerned about three key privacy issues: data misuse, unauthorized third-party sharing, and insufficient data deletion protocols. Additionally, OWASP (2021) highlights that poor data governance practices, such as vague privacy policies, lack of breach response mechanisms, and excessive data collection, remain critical risk factors. At the same time, risky user behavior, including connecting to unsecured Wi-Fi, oversharing on social media, and using weak passwords, further compromises privacy (Sangeen et al., 2023).

Despite these risks, a growing number of consumers continue to engage with businesses that use artificial intelligence and other marketing technologies to enhance speed, personalization, and convenience. In Thailand, for instance, 93% of consumers expect technology to improve service speed, and 87% believe customer experience is as important as product quality. However, 77% remain concerned about the unethical use of AI (Salesforce, 2023, as cited in TechTalkThai, 2023).

While previous studies in Thailand have examined general privacy concerns and disclosure behaviors, none have segmented consumers by their privacy personality traits. A review of the relevant literature underscores this gap. Addressing it, the present research examines the characteristics and preferences of Thai consumers across different groups in order to develop communication strategies and customer experiences via marketing technologies that align with their future willingness to disclose personal data. Accordingly, the study addresses three research questions: (1) to what extent Thai consumers are willing to disclose personal data for enhanced customer experiences through marketing technologies, (2) what levels of privacy concerns, knowledge, and behaviors they exhibit, and (3) how distinct privacy personality groups can be identified to inform communication strategies that balance customer experience with willing to disclose personal data.

Literature Review

Willingness to Disclose Personal Data

Personal data refer to any information that can directly or indirectly identify an individual, whether stored in paper or digital form. Examples include names, addresses, ID numbers, contact information, and online identifiers. Sensitive personal data, such as health status, religious beliefs, political opinions, and criminal records, poses greater privacy risks. Under Thailand's Personal Data Protection Act (PDPA), enacted in 2022, such data requires enhanced protection (Kulwanichchaiyanan, 2023; Law and Development Research Center, 2020).

In digital service environments, consumers routinely disclose personal data to access products, compare prices, or receive personalized offers. Several studies have shown that consumers are generally willing to share information when they perceive clear benefits, such as convenience, personalization, or social engagement, and when the data use appears fair and secure (Culnan & Armstrong, 1999; Crossler, 2014, as cited in Pimrabiab, 2020). However, discomfort may arise when consumers are unaware of how their data is handled, or when they sense a lack of transparency and control.

Thailand's PDPA requires organizations to obtain informed consent and provide clear privacy notices detailing data collection practices and user rights. The law aims to balance innovation and consumer protection by promoting ethical standards in data usage (Law and Development Research Center, 2020). Businesses failing to communicate these practices effectively may undermine user trust and face resistance to data sharing.

While several frameworks, including privacy calculus theory, suggest that individuals evaluate perceived benefits against privacy risks, research has found inconsistencies between stated concerns and actual behavior, a phenomenon commonly referred to as the privacy paradox. Consumer attitudes toward data disclosure are complex; they may voice concern yet still disclose information for convenience. (Knijnenburg et al., 2022)

In summary, willingness to disclose personal data is shaped by a combination of legal protection, consumer trust, perceived value, and clarity of data practices. For marketers and service providers, understanding these dynamics is crucial for designing strategies that respect privacy while enabling value-based interactions.

New Customer Experience with Marketing Technology

As marketing evolves toward greater digitalization, businesses increasingly adopt advanced technologies to create more personalized and engaging customer experiences. This shift has accelerated in the post-COVID19 era, where reliance on digital tools such as search engine

marketing (SEM), social media platforms, and e-commerce has grown significantly. Marketing Technology (MarTech) encompasses tools like artificial intelligence (AI), robotics, chatbots, and blockchain, which facilitate data-driven personalization and automation at scale.

Kotler et al. (2021) propose the 5A's Customer Path (Aware, Appeal, Ask, Act, and Advocate) as a strategic framework for designing customer engagement. In the Aware stage, customers encounter brands through digital touchpoints such as personalized ads. Appeal involves generating interest through relevant content. The Ask phase focuses on interaction, often through chatbots or inquiry systems requiring basic data disclosure. In Act, customers engage in transactions facilitated by technologies like biometric payment or AR/VR shopping. The Advocate stage emphasizes loyalty, frequently supported by AI-powered recommendation engines or reward systems.

Recent studies suggest that consumers' willingness to disclose personal data may vary across these stages, depending on the interaction context and the perceived benefit. For instance, Degutis et al. (2023) and Gupta et al. (2023) report that consumers are more willing to share data when it enables functional services, such as inquiry support or loyalty programs, than for passive exposure such as advertising.

Marketing technologies allow for extensive data collection across these stages, ranging from browsing behavior and purchase history to social media engagement and participation in brand activities. This facilitates strategies like content personalization, price optimization, and predictive targeting (Thanyarattakul, 2019). However, adoption is not universal. Kotler et al. (2021) emphasize the digital divide, which includes both access limitations and attitudinal resistance stemming from privacy concerns.

In Thailand, consumers increasingly expect faster, more personalized service from brands using modern technology. At the same time, ethical concerns, particularly regarding AI and automated decision-making, remain prevalent (Salesforce, 2023, as cited in TechTalkThai, 2023). Ensuring robust cybersecurity is essential to addressing these concerns. Principles of confidentiality, integrity, and availability are central to maintaining consumer trust (Osazuwa, 2024).

In conclusion, while MarTech offers substantial potential for enhancing customer experience, its effectiveness depends on how well businesses address privacy risks and align technological interactions with consumer expectations. Understanding how consumers respond to different stages of the customer journey can inform more responsible and effective MarTech strategies.

Online Data Privacy Personality

A growing body of research has examined how individuals perceive and respond to privacy risks in digital environments. Several theoretical frameworks have been developed to measure these differences, including the Concern for Information Privacy (CFIP) scale and the Internet Users' Information Privacy Concern (IUIPC) model. These frameworks typically assess user concerns about data collection, control, and secondary use.

Building on these, the APCO framework links privacy attitudes to outcomes such as trust, willingness to disclose, and behavior, while theories like the Privacy Calculus suggest that consumers weigh perceived benefits against privacy risks. However, this decision-making process is not always rational. The Privacy Paradox describes the inconsistency between users' stated concerns and their actual disclosure behaviors, indicating the presence of psychological and contextual influences.

To address this gap, researchers have turned to segmentation approaches based on privacy-related personality traits (see Table 1). The most widely adopted is Westin's Privacy Taxonomy (Knijnenburg et al., 2022), which classifies individuals into three groups: 1) Privacy Fundamentalists: highly protective of personal data, generally averse to disclosure, 2) Privacy Pragmatists: willing to share data when benefits outweigh risks, and 3) Privacy Unconcerned: minimally concerned and more open to data sharing.

Contemporary studies have refined these models to capture the complexity of modern digital behavior. For example, Forrester's (2022) segmentation distinguishes between groups such as Data-Savvy Digitals, Conditional Consumerists, and Reckless Rebels, based on privacy knowledge, behavior, and attitudes. Similarly, Schomakers et al. (2019) propose categories like Privacy Guardians, Pragmatists, and Cynics, while Morton and Sasse (2014) emphasize dimensions such as trust, information control, and perceived benefits.

Table 1: Previous Privacy Personality Conceptualizations

Authors (Year)	Privacy Factors	Privacy Personality	
Westin's Privacy Taxonomy	Knowledge & Preference	3 groups:	(1) Privacy Fundamentalists (2) Privacy Pragmatists (3) Privacy Unconcerned
Morton & Sasse (2014)	Organizational, Technology lens, Other Factors	5 groups:	(1) Information Controller (2) Security Concerned (3) Benefits Seekers (4) Crowd Followers (5) Organizational Assurance Seekers
Schomakers et al. (2019)	Concern & Behavior	3 groups:	(1) Privacy Guardian (2) Privacy Cynic (3) Privacy Pragmatist
Biselli et al. (2022)	Knowledge & Behavior	3 groups:	(1) Privacy Fundamentalists (2) Privacy Pragmatists (3) Privacy Unconcerned *(same as Westin's Privacy Taxonomy)*
Forrester (2022)	Willingness to Share information, Privacy Awareness, Comfort with the Data Economy, Protective Behaviors	5 groups:	(1) Reckless Rebels (2) Conditional Consumerists (3) Data-Savvy Digitals (4) Nervous Unawares (5) Skeptical Protectionists
Cisco (2023)	Care, Willing to protect, Switched brands	Percentage (%) of Privacy Active	

These segmentation models offer practical value for marketers and researchers seeking to personalize data governance and communication strategies. They reflect the reality that consumers are not a homogeneous group but differ significantly in their expectations, behaviors, and levels of knowledge regarding online privacy.

The literature review on related issues reveals that while some research in Thailand has addressed privacy concerns and the disclosure of personal data, no study has yet classified Thai consumers based on privacy personas. Furthermore, with stricter enforcement of the Personal Data Protection Act (PDPA) and growing consumer concerns, access to customer data has become more difficult. Meanwhile, demand for new marketing experiences is rising, making marketing technologies vital for managing data and enabling effective data-driven marketing strategies. These factors motivated this study, which applies the Internet User Privacy Concern Scale (IUIPC) by Groß (2021, as cited in Gerber et al., 2023) and Westin's Privacy Taxonomy as adopted in Biselli et al.'s (2022) research to categorize online data privacy personality, along with the 5A's Customer Path and Marketing Technology model (Kotler et al., 2021) to find opportunities to make consumers willing to disclose personal data.

Methodology

This study is quantitative research conducted with Thai consumers aged 18-59 (born between 1965 and 2006) who regularly use the internet and interact with businesses using marketing technologies. Due to the unknown population size, a sample of at least 400 was determined using a 95% confidence level and a .05 margin of error. The sample was selected through snowball and accidental sampling, with screening questions used to ensure relevance.

Data were collected via an online self-administered questionnaire on Microsoft Forms, distributed through LINE and Facebook between March and April 2024. The questionnaire consisted of closed-ended items developed from relevant theories and literature, reviewed by experts, and approved by the Institutional Review Board (IRB). It comprised six sections: 1) screening questions, 2) online data privacy concern (10 items), 3) online data privacy knowledge (20 items), 4) online data privacy behaviors (12 items), 5) willingness to disclose personal data (17 items), and 6) demographic information. Reliability was assessed using Cronbach's Alpha, yielding values between .717 and .918.

For data analysis, descriptive statistics cover frequency, percentage, mean, and standard deviation. Factor Analysis, using Principal Component Analysis with Varimax rotation, was applied to reduce the number of variables by grouping related items. Finally, K-means Cluster Analysis was used to segment consumers by online privacy personality.

Findings

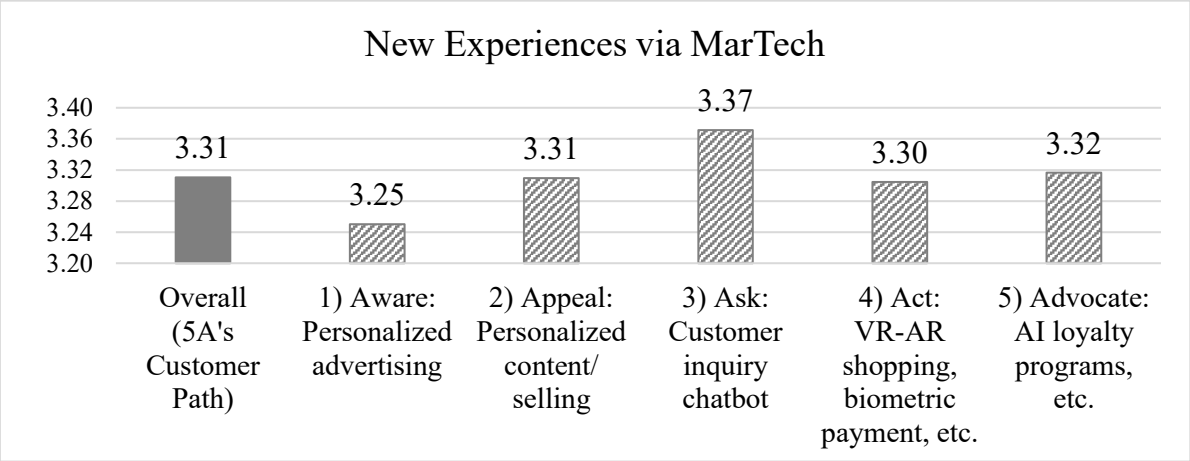
The demographic analysis reveals an equal distribution of male and female samples with an average age of 35. A majority hold a bachelor's degree (62.86%) and spend over five hours daily on the Internet (86.19%). The most frequently used platforms are Line (60.24%), followed by entertainment platforms such as Netflix, Spotify, and Garena ROV (53.33%), YouTube (40.71%), and TikTok (30.48%).

Additionally, most samples have academic or professional experience in market research and data analysis (52.38%), technology and computer programming (50.95%), and digital marketing and communications (50.71%). All samples utilized business services employing marketing technologies, particularly artificial intelligence (100.00%). Most had also engaged with other technologies, including natural language processing (84.52%), robotics (72.62%), and sensor tech (63.33%).

Willingness to Disclose Personal Data

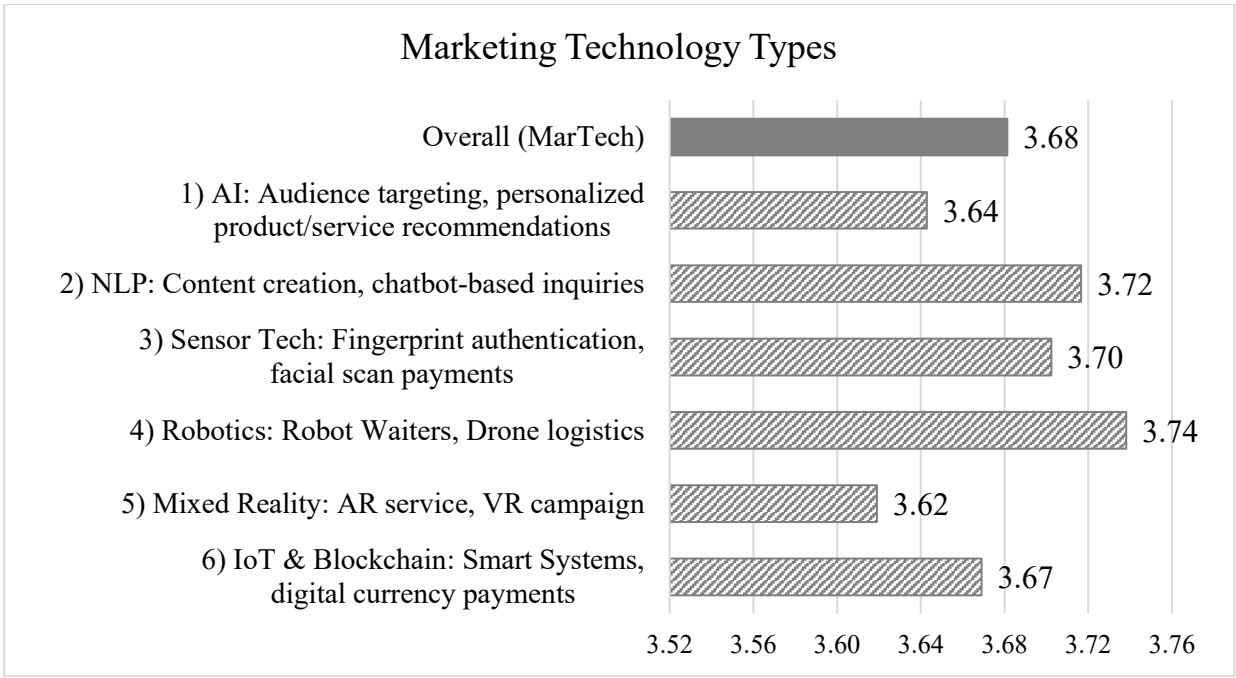
The analysis of the samples' willingness to disclose personal information reveals a willingness to share personal data for new experiences through marketing technologies at a moderate level (M = 3.31, SD = 1.15). Samples are particularly willing to disclose information for the "Ask" phase of customer experiences (M = 3.37, SD = 1.28), such as customer inquiries handled by chatbots. However, for new customer experiences, the samples are willing to disclose their data the least for the "Aware" phase (M = 3.25, SD = 1.25), such as personalized advertising (Songja & Cheyjunya, 2024), as detailed in Figure 1.

Figure 1: Willingness to Disclose Personal Data by New Experience Types via MarTech



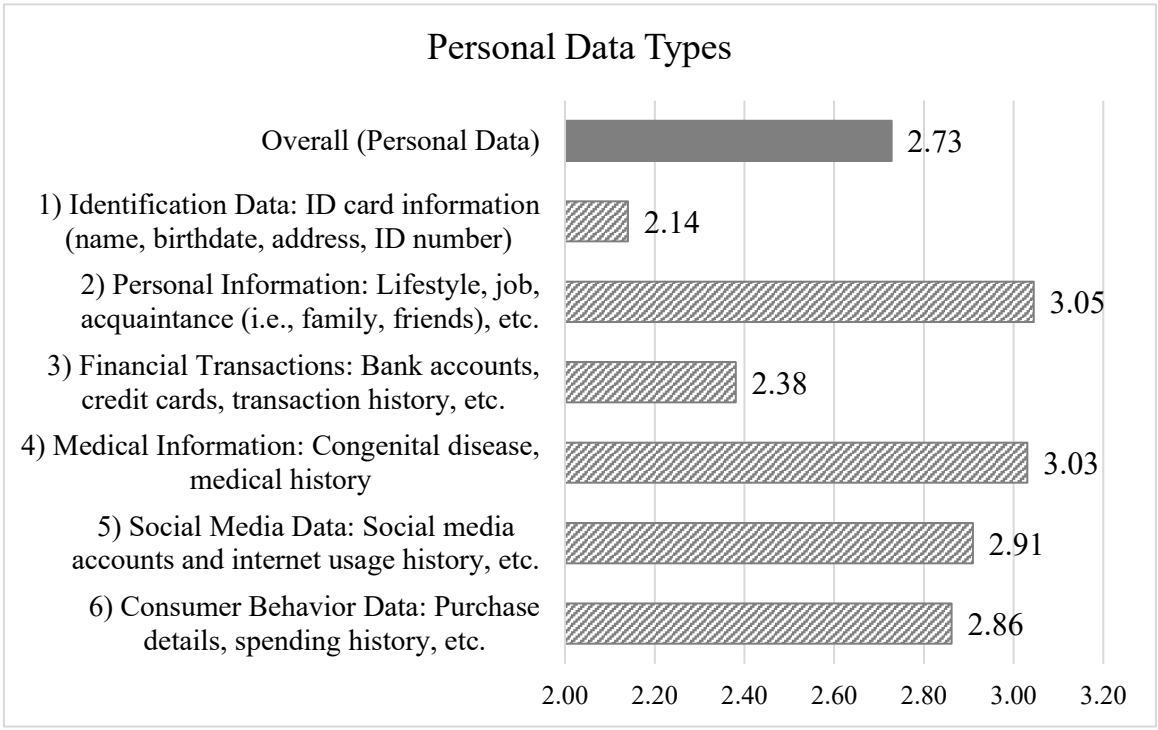
Regarding the types of marketing technology, the samples generally show willingness to disclose data of all types at a high level (M = 3.68, SD = 0.87), with the highest willingness for robotics (M = 3.74, SD = 1.01), natural language processing (NLP; M = 3.72, SD = 1.03), and sensor tech (M = 3.70, SD = 1.00). In contrast, willingness for mixed reality (AR or VR; M = 3.62, SD = 1.05) and artificial intelligence (AI; M = 3.64, SD = 1.07) is at the lowest level, compared to other types of technology (Songja & Cheyjunya, 2024). as shown in Figure 2.

Figure 2: Willingness to Disclose Personal Data by Marketing Technology Types



Regarding the types of personal (Songja & Cheyjunya, 2024), the samples are willing to disclose their overall personal data at a moderate level (M = 2.73, SD = 1.01). Specifically, the samples are willing to disclose personal, lifestyle, and acquaintance information as well as medical data, congenital disease, and medical history, the most (M = 3.05, SD = 1.16, and M = 3.03, SD = 1.23, respectively). However, they are the least willing to disclose such information if it is related to their ID data and financial transaction information (M = 2.14, SD = 1.12 and M = 2.38, SD = 1.26, respectively), as shown in Figure 3.

Figure 3: Willingness to Disclose Personal Data by Personal Data Types



Online Data Privacy Concern

The samples exhibit online privacy concerns at the highest level (M = 4.27, SD = 0.69), especially regarding awareness of data usage (M = 4.32, SD = 0.74). They emphasize wanting to know which of and how their personal data is being used (M = 4.34, SD = 0.81) and believe that service providers who want to collect online data should inform them about what data is collected and its intended use (M = 4.33, SD = 0.82).

Online Data Privacy Knowledge

The samples exhibit knowledge of online data privacy risks at a high level (M = 3.92, SD = 0.63). The top three issues they know are the possibility of providers collecting personal data for marketing or sharing it with third parties (M = 4.24, SD = 0.92), unauthorized data collection by others during online usage (M = 4.21, SD = 0.82), and the risk of data theft (M = 4.16, SD = 0.88).

Conversely, the issues the samples know the least are risks related to trust in providers' data protection policies (M = 3.28, SD = 1.29), using search engines usage that may threaten privacy (M = 3.71, SD = 1.17), and the use of a single password for all accounts or logging in with Facebook, Line or email usernames (M = 3.75, SD = 1.19), which are 3 issues that may cause the samples to unknowingly violate their privacy.

At the same time, they know their privacy rights and protection at a high level (M = 4.11, SD = 0.64), The three issues that the samples know the most are the right to object to the collection, use, or disclosure of personal information about them at any time (M = 4.36, SD = 0.79), the right to request the deletion, destruction, or anonymization of their personal information (M = 4.24, SD = 0.86), and adjusting their own social media privacy settings to disclose less personal information (M = 4.23, SD = 0.81).

However, they still have low knowledge of some issues, especially the right to know the purposes of collecting or using one's personal data from the service provider (M = 3.75, SD = 1.22), the right to request access, receive a copy, or transfer personal data about oneself that the service provider has collected (M = 4.01, SD = 0.96), and the methods of protecting data by rejecting cookies or regularly deleting the history of browsing on the website (M = 4.05, SD = 0.94).

Online Data Privacy Behavior

The samples report risk behaviors at a moderate level (M = 2.69, SD = 0.50), by frequently using search engines (such as Google) without hesitation in terms of privacy (M = 3.80, SD = 1.05) and using the same password for all their online accounts or logging in with their Facebook, Line, or email usernames (M = 3.18, SD = 1.28), which are the two behaviors that increase privacy risks the most.

On the other hand, it is found that the samples exhibit protective behaviors at a low level (M = 2.26, SD = 0.80). Namely, the preventive behaviors they often perform are "reading data protection and private policies thoroughly before agreeing to use online services." (M = 2.53, SD = 1.10) and “deleting browsing history on websites or applications.” (M = 2.40, SD = 1.10). Furthermore, using a VPN when accessing websites via public networks is the samples' least protective behavior. (M = 1.94, SD = 1.04).

Online Data Privacy Personality

The analysis combined privacy concerns, knowledge, and behaviors, applying Principal Component Analysis (Varimax rotation) to 35 variables. The KMO value was 0.945 (> 0.50) and Bartlett’s Test yielded a Chi-square value of 7904.361 (p < .001), confirming suitability for factor analysis. Six factors were extracted, explaining 61.09% of the variance (see Tables 2 and 3).

Table 2: The number of Factors, Eigenvalues, Percentage of Explained Variance, and Cumulative Percentage of Variance

	Factor	Eigenvalue	% of Variance	Cumulative %
1	Data Collection Awareness	12.326	35.216	35.216
2	Data Control	3.427	9.790	45.007
3	Internet Risk	1.914	5.469	50.475
4	Policy Understanding	1.521	4.346	54.822
5	Proactive Protection	1.229	3.512	58.334
6	Convenience	0.963	2.752	61.086

Table 3: Definitions, Characteristics, and Factor Loadings of Six Factors

Factor	Item Loading
1) Data Collection Awareness *A group of factors related to consumers' awareness of service providers' personal data collection and concerns over potential impacts caused by such collection consists of 11 items.*	
I am concerned that online platforms are collecting too much of my personal data unnecessarily.[C]	0.560
I agree that service providers collecting information online should inform the data subjects about the way the data is collected, processed, and used.[C]	0.558
It usually bothers me when online platforms request my data before I receive services.[C]	0.552
It bothers me to share my personal data with so many online platforms.[C]	0.550
I know others may attempt to collect my personal data during online usage without permission.[C]	0.542
I know I have the right to access, request a copy, or transfer my personal data that service providers have collected from the online platforms I use.[K]	0.536
When online platforms ask me for personal data, I sometimes think twice before providing it.[C]	0.510
I agree that a good Privacy Policy should have a clear, visible, and conspicuous disclosure on websites or applications.[C]	0.507
I believe that online privacy is invaded when I lose control or unwillingly have reduced control.[C]	0.493
I know I am at risk of becoming a victim of personal data theft when using online platforms.[K]	0.445
I know I have the right to request that my personal data be corrected to be accurate and complete from the service providers I use online platforms.[K]	0.419
2) Data Control *A group of factors related to consumers' desire and ability to control access to and use their personal data on the internet. It consists of 9 items.*	
I know I have the right to object to the collection, use, or disclosure of my personal data at any time from the service providers I use online platforms.[K]	0.568
I know I should adjust the privacy settings on my social media (i.e., Facebook) to disclose fewer personal data.[K]	0.532
I want to know what my personal data is used for.[C]	0.522
I agree that consumer control of personal data lies at the heart of consumer privacy.[C]	0.502
I agree that online privacy is the consumer's right to control and decide how their data is collected, used, and shared with others.[C]	0.492
I know that accessing multiple platforms simultaneously can cause the risk that others may use my personal data without permission.[K]	0.464
I know I have the right to request the deletion, destruction, or anonymization of my personal data from the service providers when I use online platforms.[K]	0.459
I post a lot of personal photos or videos on social media (e.g., Facebook, TikTok, Instagram) without setting the posts to friends-only or private.	-0.456
I know I should read the data protection and privacy regulations before registering with an online service.[K]	0.408

Factor	Item Loading
3) Internet Risk *A group of factors related to consumers' knowledge and behaviors that may expose privacy risks during internet usage. It consists of 5 items.*	
I know I can use the same password for all online accounts or log in with Facebook, Line, or email username.[K]	0.778
I know that using search engines does not threaten my privacy.[K]	0.745
I know I can protect my personal data by rejecting cookies or regularly deleting browsing history on websites.[K]	0.595
I use the same password for all my online accounts or sign in with my Facebook, Line, or email username.[B]	0.528
I know that service providers can collect my personal data for marketing purposes and share it with third parties.[K]	0.507
4) Policy Understanding *A group of factors related to consumers' understanding and trust in service providers' data management policies. It consists of 2 items.*	
I know that for the online platforms I use, I have the right to be informed by the service providers about the purpose of collecting or using my personal data.[K]	0.786
I know I can trust the data protection measures and privacy policies of the service providers when I use online platforms.[K]	0.660
5) Proactive Protection *A group of factors related to consumers' behaviors or methods for using technologies to protect online privacy. It consists of 5 items.*	
I use privacy control programs or applications (e.g., ad-blocking apps and antivirus software with privacy protection mode).[B]	0.704
When using a public network, I surf via a VPN (Virtual Private Network) connection.[B]	0.691
I delete my browsing history on websites or applications.[B]	0.656
I use search engines without hesitation (in terms of my privacy).[B]	-0.656
I read the data protection and privacy regulations before registering with an online service.[B]	0.608
6) Convenience *A group of factors related to the trade-off between the convenience provided by service providers and the potential for consumers' privacy risks. It consists of 3 items.*	
I accept cookies immediately without reading details or adjusting settings as needed.[B]	0.769
I provide my data in exchange for online access, activities, or benefits that I want or am interested in.[B]	0.737
I log into my personal email, social media, or online bank accounts via public Wi-Fi (e.g., while traveling, or in cafes).[B]	0.531

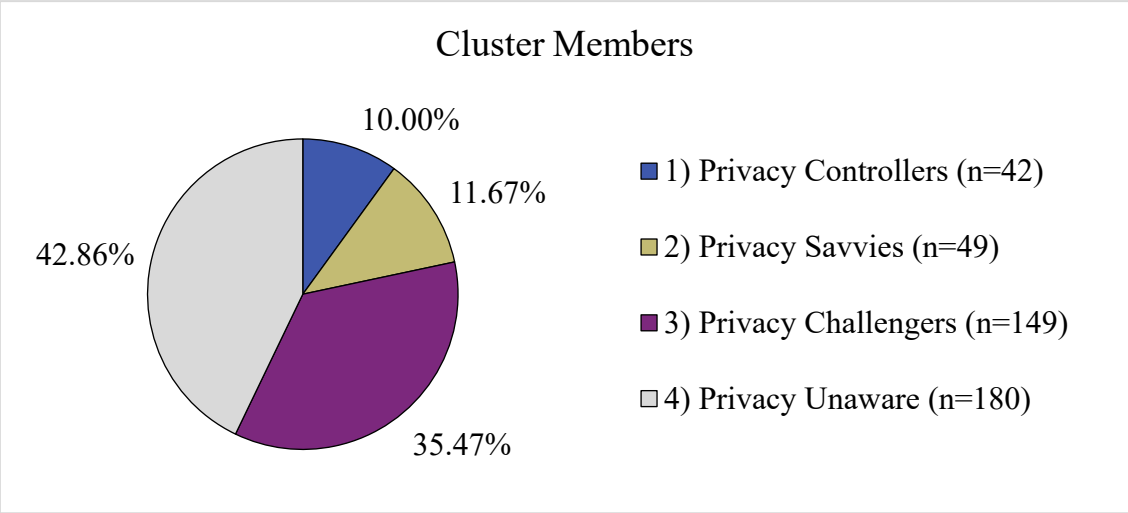
Note: [C] = Concern, [K] = Knowledge, and [B] = Behavior

Using these factors, K-means cluster analysis identified four distinct personality groups with significant differences ($p < .05$) (see Table 4 and Figure 4). The largest was Cluster 4, which consists of a total of 180 members (42.86%) of the samples.

Table 4: ANOVA Analysis of K-Means Cluster Analysis

	Factor	Cluster		Error		*F*	*p*
		Mean Square	df	Mean Square	df		
1	Data Collection Awareness	19.470	3	0.867	416	22.462	.000
2	Data Control	62.734	3	0.555	416	113.076	.000
3	Internet Risk	60.833	3	0.569	416	107.004	.000
4	Policy Understanding	64.314	3	0.543	416	118.352	.000
5	Proactive Protection	3.371	3	0.983	416	3.430	.017
6	Convenience	20.556	3	0.859	416	23.931	.000

Figure 4: Number and Percentage of Members in Each Cluster

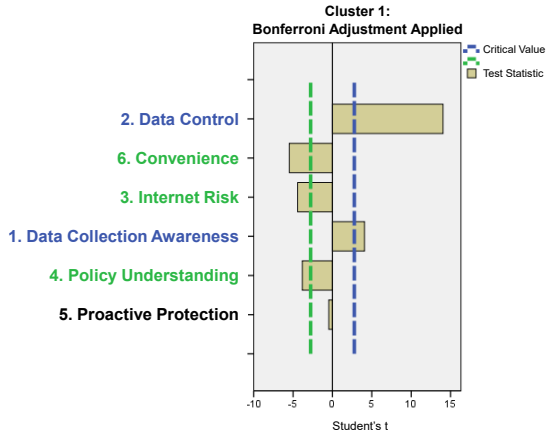


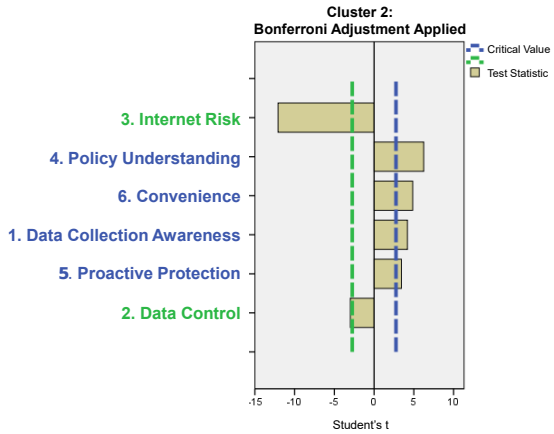
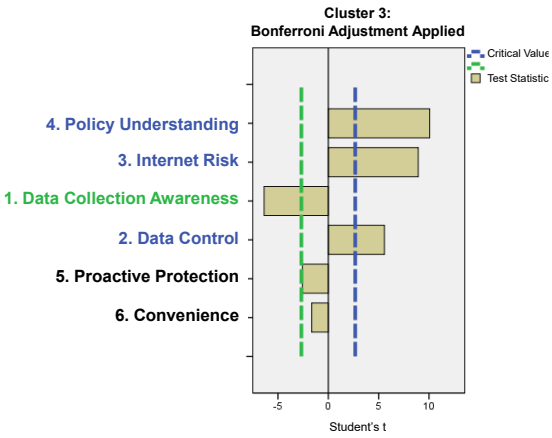
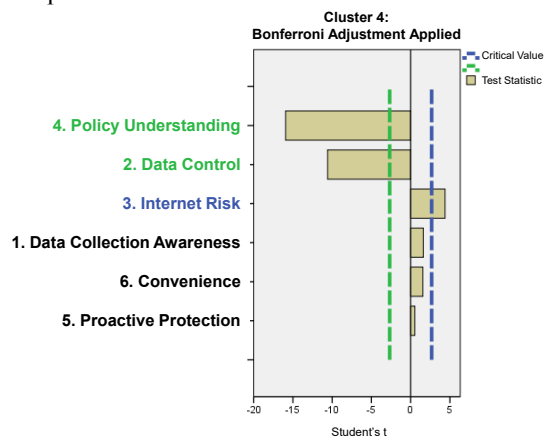
To further interpret these results, the standardized mean values from each cluster were examined to identify and rank unique traits for the online data privacy personality types (see Table 5). A subsequent Variable Importance Analysis highlighted the most influential variables within each group (see Table 6).

Table 5: Final Cluster Centers

	Factor	Cluster			
		1) Privacy Controllers	2) Privacy Savvies	3) Privacy Challengers	4) Privacy Unaware
1	Data Collection Awareness	0.494	0.534	-0.460	0.120
2	Data Control	1.615	-0.395	0.337	-0.548
3	Internet Risk	-0.823	-1.517	0.470	0.216
4	Policy Understanding	-0.495	0.907	0.647	-0.667
5	Proactive Protection	-0.059	0.348	-0.156	0.048
6	Convenience	-0.810	0.781	-0.137	0.090

Table 6: Key Traits of Each Online Data Privacy Personality Group

Cluster	Variable Importance Analysis
1) Privacy Controllers *This group prioritizes controlling access to and the use of their personal information on the internet. They do not exchange their personal data for the convenience of online services. While they have a fair understanding of safe internet practices and are aware of data collection processes, they remain skeptical of service providers' privacy policies and data handling purposes. As a result, they are likely to be less willing to disclose their information compared to other groups.*	5 Importance factors: 

Cluster	Variable Importance Analysis
2) Privacy Savvies *Members of this group have the highest understanding of service providers' privacy policies and are willing to trade some privacy for online service convenience. They do not emphasize strict control over access to their personal data, yet they are the least likely to face privacy violations. They possess safe internet usage knowledge, are aware of data collection processes, and employ current privacy-protection technologies. Thus, they are open to sharing their data voluntarily. If the service offering aligns with their needs.*	6 Importance factors: 
3) Privacy Challengers *This group is at the highest risk of experiencing privacy intrusions online. They feel limited concern about data being collected and have a basic understanding of privacy policies and data management options. Although members have some knowledge of controlling their personal data, they often share information online without fully considering the implications. As a result, they may disclose personal data both consciously and inadvertently.*	4 Importance factors: 
4) Privacy Unaware *Members of this group have the least understanding of service providers' privacy policies and minimal knowledge of personal data control techniques. They are highly vulnerable to privacy breaches due to low knowledge and limited safe internet practices. This group might unknowingly disclose their personal data and may feel uncomfortable. If they are aware that their data has been used.*	3 Importance factors: 

Discussions

Willingness to Disclose Personal Data

The study finds that the samples are willing to disclose personal data for new experiences enabled by marketing technology at a moderate level, especially in the "Ask" phase of the 5A's Customer Path, such as answering customer questions with a chatbot system, and the lowest in the "Aware" phase involving personalized advertising. This finding aligns with Liu et al. (2023), who show that chatbot interactions framed in functional communication contexts significantly increase users' willingness to self-disclose, and with Forbes' (2023) marketing trends report highlighting the role of AI marketing automation, particularly AI-driven chatbots, in creating personalized customer interactions and fostering stronger customer relationships. In the Thai context, Wutthiphaphinyo (2021) confirms

that the quality and usability of chatbot services positively affect satisfaction and trust, leading to greater willingness to disclose information.

Conversely, Leszczynska and Baltag (2024) report that consumers are generally reluctant to share personal data for personalized advertisements, even when the service is perceived as beneficial, due to privacy concerns and the unsolicited nature of such targeting. Supporting this, Buvaneswari and Swetha (2024) show that perceived intrusiveness in targeted advertising significantly increases ad avoidance and reduces willingness to disclose personal information. Likewise, Chotimanon's (2021) study on targeted online advertising in Thailand highlights that such advertising can access and collect consumers' personal data, emphasizing the need for businesses to prioritize consumer data security.

Regarding the types of marketing technologies, the samples are willing to disclose at a high level, especially for robotics, natural language processing (NLP), and sensor technology. This preference is consistent with some marketing trends in 2024 that Forbes (2023) has compiled, including the AI Marketing Automation trend that uses chatbots to increase the efficiency of customer interactions and the Voice Search Optimization trend that increases the efficiency of voice search to find the desired content better. And with NECTEC's (2023) report on the rapid growth of the service robotics market in Thailand, driven by demand in healthcare, hospitality, and logistics amid labor shortages and an ageing population.

By contrast, willingness is lower for mixed reality (MR) and artificial intelligence (AI). Sung et al. (2021) show that while these technologies can enhance engagement through immersive and personalized experiences, they also raise substantial concerns over data privacy and tracking, which can reduce users' willingness to disclose personal information. Similarly, TrustArc's (2024) analysis notes that features such as continuous spatial mapping, behavioral tracking, and integration with third-party systems increase the risk of unauthorized data use, reinforcing user hesitancy to share personal data.

In terms of data types, the samples are willing to disclose information overall at a moderate level. The highest willingness is found for personal data, lifestyle, acquaintance, and health-related information (e.g., congenital diseases or ongoing conditions, medical history, etc.) However, the least willingness is for information on the national ID card and financial transaction data. This is consistent with Denpaisan's (2009) study on the influence of privacy attitudes on internet users' trust in websites, which finds that internet users are more willing to disclose demographic and lifestyle information but are more cautious with personally identifiable and financial data. It also supports Dokphrom's (2015) study on Facebook privacy awareness, which indicates that the types of personal data most disclosed are institutional data, date of birth, and interest-based information. Additionally, Rojananark et al.'s (2021) research on health wearables shows a positive correlation between intent to use and willingness to share health data at a statistically significant level.

Online Data Privacy Concern

It is found that the samples exhibit the highest level of concern about online data privacy, particularly regarding awareness of how their data is used. They want to know the specific purposes for which their personal data is collected and to receive clear communication from service providers about what data is gathered and how it will be utilized. This aligns with Denpaisan's (2009) study on the influence of privacy attitudes on internet users' trust in websites, which indicates that Thai internet users show a high level of privacy concern, with the greatest emphasis on how their data is collected and used. Similarly, Cisco's (2020) survey reports that 60% of consumers are concerned about the protection of their personal data, and one of the main issues is that service providers' data use does not align with the intended purposes. Supporting this, Rosário and Dias (2023) highlight that privacy concerns remain a major challenge for data-driven marketing initiatives.

Online Data Privacy Knowledge

The findings show that the samples demonstrate a high level of knowledge regarding online data privacy risks. They are most aware that service providers may collect personal data for marketing purposes or share it with third parties, recognize the possibility of unauthorized data collection by others during online service use, and perceive the risk of personal data theft. These results align with the Law and Development Research Center (2020), which describes privacy risks in marketing as involving two main purposes: tracking to better understand consumers' identity and needs, and targeting them directly for marketing. Data collection by either direct or third-party sources poses moderate-to-high risks, while direct targeting for advertising or sales carries a high risk of privacy invasion. Frequently, targeted marketing uses both personal identity data (e.g., age, gender, education, occupation, residence) and observed behavioral data (e.g., peer groups, purchase history, online interactions). Similarly, OWASP (2021) identifies risks from poor operational practices of service providers, including operator-sided data leakage, inadequate breach

response, non-transparent policies, excessive data collection, and third-party sharing, all of which increase the likelihood of data theft without consumer awareness.

Conversely, the samples have the least knowledge about risks related to service providers' data security measures, privacy threats from search engine use, and the use of identical passwords or social media logins (e.g., Facebook, Line, email). These gaps correspond with recommendations from Wuttidittachotti et al. (2021) and Panda Security (2023), which emphasize avoiding the same password across systems, refraining from social media logins, and using privacy-focused search engines. For example, Google retains search queries and related data to improve its algorithms and enable targeted marketing, creating potential privacy risks. Pattanavijit (2015) further supports this by showing that knowledge of these risks influences users' willingness to disclose personal data via social media logins.

The samples also show a high level of knowledge regarding personal data rights and preventive measures. They are most aware of the right to object to data collection, use, or disclosure at any time; the right to request deletion or anonymization; and the ability to adjust social media privacy settings to limit disclosure. These findings align with Ramasoota and Panichpapiboon (2013), who note that users often adjust privacy settings in parallel with legal and regulatory measures. Similarly, Dokphrom (2015) finds that Facebook users are aware of privacy settings and frequently restrict visibility to known contacts.

However, there are areas where knowledge is lower, such as the right to know the purpose of data collection, the right to request access or transfer of personal data, and privacy protection methods like rejecting cookies or clearing browsing history. These gaps are consistent with Wuttidittachotti et al. (2021), who call for enhanced security awareness and user skills to monitor and manage personal data. They also indicate misalignment with Thailand's Personal Data Protection Act (PDPA) of 2019, which requires service providers to inform consumers through a privacy notice detailing the types of data collected, purposes of collection, and data owner rights, including the right to be informed, the right of access, and the right to data portability.

Online Data Privacy Behavior

The study shows that the samples display risky online behaviors at a moderate level. The behaviors most likely to increase privacy risks are the frequent use of search engines (e.g., Google) without privacy considerations and the use of the same password across multiple accounts or social media logins (e.g., Facebook, LINE, email). These results are consistent with earlier findings on their least awareness of certain privacy risks and align with the recommendations of Wuttidittachotti et al. (2021) and Panda Security (2023), which emphasize selecting privacy-focused search engines. Google's collection of search queries and user interests to support targeted marketing can compromise privacy. Similarly, using the same password or relying on social media logins increases vulnerability, as supported by Pattanavijit's (2015) finding that the perceived convenience of such logins encourages adoption, despite the added risk.

Regarding protective behaviors, the samples show a low level of preventive action, with only occasional review of privacy terms before acceptance and occasional deletion of browsing history. VPN usage is the least common protective behavior. These results align with Chotimanon's (2021) research, which finds that most users do not fully review privacy policies before consenting. Boerman et al. (2021) also note that actions like deleting browser history are performed inconsistently, though this is one of the more common preventive measures among the samples. Recommendations by Panda Security (2023) further stress the importance of VPNs for masking IP addresses and securing browsing activities, particularly on public Wi-Fi.

Online Data Privacy Personality

This study identifies six online data privacy personality factors through factor analysis: data collection awareness, data control, internet risk, policy understanding, proactive protection, and convenience. These factors align to varying degrees with Westin's Privacy Taxonomy (Westin, 1967 as cited in Knijnenburg et al., 2022) and its later interpretations (Austin, 2019; Hoofnagle & Urban, 2014), as well as with newer segmentation frameworks (Forrester, 2022; Morton & Sasse, 2014; Schomakers et al., 2019).

Data collection awareness and *data control* correspond to the traits of *Privacy Fundamentalists* and *Privacy Pragmatists* in Westin's framework, reflecting informed evaluation of data flows and selective disclosure (Austin, 2019; Hoofnagle & Urban, 2014). These also align with the *Organization, Information Management, and Information Principles* categories in Morton and Sasse (2014), the *Awareness* and *Privacy self-efficacy* factors in Forrester (2022), and Schomakers et al.'s (2019) segmentation, individuals with strong control and awareness are classified as *Data-Savvy Digitals*, who prioritize privacy safeguards and data governance.

Similarly, *internet risk* and *policy understanding* relate to Westin's *reserve* and *anonymity* constructs (Hoofnagle & Urban, 2014),

which focus on reducing identifiability and maintaining informational distance, consistent with *Consequences for Individual* and *Protection* in Morton and Sasse (2014) and with *Privacy concern, Trust in online companies,* and *Need for privacy* in Schomakers et al. (2019).

In contrast, *convenience* reflects a willingness to trade aspects of privacy for usability benefits while still considering risks and rewards. This is in line with *Privacy Pragmatists* in Westin's taxonomy (Austin, 2019), *Benefits for Individuals* in Morton and Sasse (2014), and the *Privacy Pragmatist* type in Schomakers et al. (2019).

Proactive protection, meanwhile, extends beyond the attitudinal scope of Westin's original model, referring to the active use of technological tools such as VPNs, password managers, and ad-blocking software. It aligns with *Protection* and *Technology Features* in Morton and Sasse (2014), *Privacy protection behavior* in Schomakers et al. (2019), and *Protective Behaviors* in Forrester (2022).

Using these six factors, four distinct online privacy personality groups were identified: Privacy Controllers (10.00%), Privacy Savvies (11.67%), Privacy Challengers (35.47%), and Privacy Unaware (42.86%). These align with Westin's Privacy Taxonomy (Knijnenburg et al., 2022) and other models (see Table 7). For instance, *Privacy Controllers* in this study resemble Westin's *Privacy Fundamentalists* and Forrester's *Data-Savvy Digitals*. They maintain a strong privacy commitment and share personal information only when required, prioritizing control, transparency, and data minimization in their interactions.

By contrast, *Privacy Unaware* differs significantly from Westin's *Privacy Unconcerned*. While the latter are generally unconcerned about privacy and willing to share personal data freely, *Privacy Unaware* in this study show concern about privacy but lack the knowledge and skills to protect it. This makes them more vulnerable to breaches and unintentional disclosure. Their profile is closer to Forrester's *Nervous Unawares*, who are cautious yet have limited capability to manage privacy effectively.

Table 7: Similar Characteristics in Grouping Consumer Privacy Personality, Compared with Related Theories and Studies

Previous Consumer Privacy Personality	**Four Clusters of Online Data Privacy Personality**			
	1) Privacy Controllers *High Privacy: Reluctant to share data*	**2) Privacy Savvies** *Willing to share, weighing risks and benefits*	**3) Privacy Challengers** *Low Concern: Freely shares data*	**4) Privacy Unaware** *Concerned but lacks knowledge*
Westin's Privacy Taxonomy	Privacy Fundamentalists	Privacy Pragmatists	Privacy Unconcerned	
Morton & Sasse (2014)	Information Controller	Benefits Seekers		
Schomakers et al. (2019)	Privacy Guardian	Privacy Pragmatist	Privacy Cynic	
Forrester (2022)	Data-Savvy Digitals	Conditional Consumerists	Reckless Rebels	Nervous Unawares

Understanding these distinctions provides a clear foundation for tailoring communication, consent mechanisms, and privacy protection strategies to each group's attitudes and capabilities. Figure 5 integrates demographic profiles with each segment's willingness to share personal data across categories, customer experiences, and marketing technologies. This persona-based framework links statistical segmentation to practical strategies for privacy communication and consent, enabling organizations to encourage informed and voluntary data sharing while maintaining trust and compliance.

Consent or privacy notice suggestions for each persona group:

1. Privacy Controllers: Respond well to consent notices emphasizing transparency, granular control, and data minimization (Bruhner et al., 2023).

2. Privacy Savvies: Can be engaged through concise, salient privacy notices that clearly communicate mutual value exchange (Ebert et al., 2021; Ding, 2024).

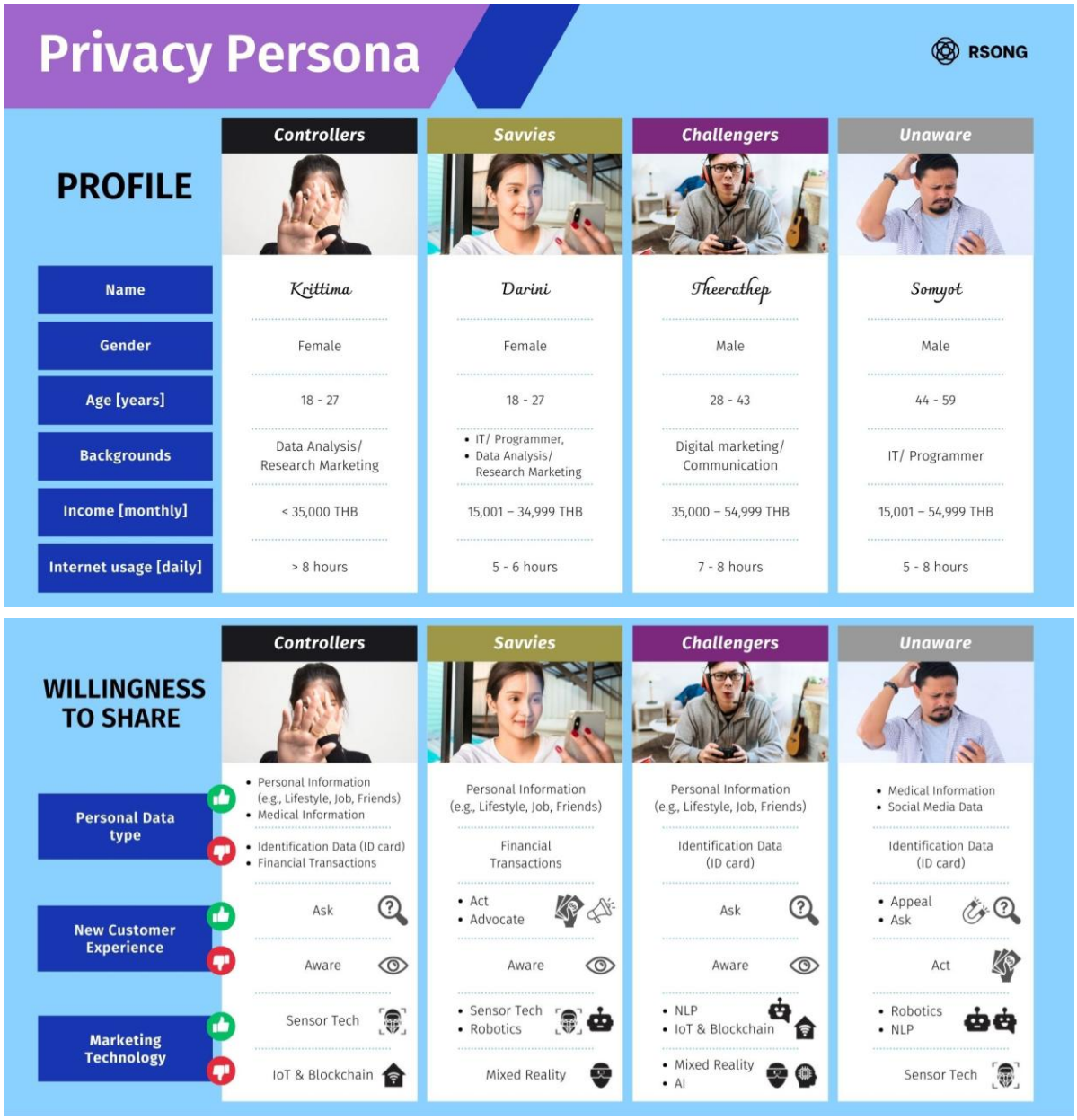
3. Privacy Challengers: Benefit from simplified, benefit-oriented notices that avoid

manipulative consent designs, addressing the effects of "dark patterns" (Nouwens et al., 2020).

4. Privacy Unaware: Require layered, visually guided consent frameworks supplemented by educational prompts to build baseline privacy literacy (Syrmoudis, 2024).

Integrating these consent and privacy notice approaches into marketing technology strategies can enhance trust, support regulatory compliance, and strengthen long-term consumer relationships across all privacy personality segments.

Figure 5: Privacy Personas and Their Willingness to Share Personal Data for Improved Customer Experiences via Marketing Technology



Limitations

The study's Thai sample offers context-specific insights but limits generalizability. Cross-cultural comparisons could assess the universality of the factors and segments. The online self-administered questionnaire provided broad coverage but may have been affected by recall bias or social desirability.

Future studies could incorporate behavioral or experimental methods to observe actual data-sharing practices. The segmentation model, based on factor analysis and clustering, is practical but would benefit from validation with larger and more diverse samples. Lastly, while

suggestions for consent and privacy notice design are proposed, their real-world effectiveness requires empirical testing in future research.

ORCID ID

Patchanee Cheyjunya: https://orcid.org/0009-0000-5809-5426

References

Austin, L. M. (2019). Re-reading Westin. *Theoretical Inquiries in Law, 20*(1), 53-86. https://doi.org/10.1515/TIL-2019-0003

Biselli, T., Steinbrink, E., Herbert, F., Schmidbauer-Wolf, G. M., & Reuter, C. (2022). On the challenges of developing a concise questionnaire to identify privacy personas. In *Proceedings on Privacy Enhancing Technologies, 2022*(4), 645-669. https://doi.org/10.56553/popets-2022-0126

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research, 48*(7), 953-977. https://doi.org/10.1177/009365021880091

Bruhner, C. M., Hasselquist, D., & Carlsson, N. (2023). Bridging the privacy gap: Enhanced user consent mechanisms on the web. *Internet Society*, 1-13. https://dx.doi.org/10.14722/madweb.2023.23017

Buvaneswari, P. S., & Swetha, M. S. (2024). AD avoidance in digital advertising: The impact of privacy disruption and perceived intrusiveness. In *Proceedings of the International Conference on Digital Transformation in Business: Navigating the New Frontiers Beyond Boundaries (DTBNNF 2024)* (pp. 57-76). https://doi.org/10.2991/978-94-6463-433-4_6

Chotimanon, P. (2021). Privacy issues in the case of targeted online advertising. *Ramkhamhaeng Law Journal, 11*(2), 51-78. https://so05.tci-thaijo.org/index.php/lawjournal/article/view/262966/177033

Cisco. (2020). *Cisco 2020 Consumer privacy survey*. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-infographic-2020.pdf

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104-115. https://doi.org/10.1287/orsc.10.1.104

Degutis, M., Urbonavičius, S., Hollebeek, L., & Anselmsson, J. (2023). Consumers' willingness to disclose their personal data in e-commerce: A reciprocity-based social exchange perspective. *Journal of Retailing and Consumer Services, 74*, 1-28. https://doi.org/10.1016/j.jretconser.2023.103385

Denpaisan, P. (2009). *The Influence of internet users' privacy attitudes on website trust.* [Master's thematic paper, Thammasat University]. TU Digital Collections. https://digital.library.tu.ac.th/tu_dc/frontend/Info/item/dc:119771

Ding, X. (2024). For whom is privacy policy written? A new understanding of transparency. *International Data Privacy Law, 14*(3), 197-211. https://doi.org/10.1016/j.clsr.2024.106072

Dokphrom, P. (2015). Awareness of information privacy on online social networking sites of students at the Faculty of Arts, Silpakorn University: A case study of Facebook. *Veridian E-Journal, Silpakorn University (Humanities, Social Sciences and Arts), 8*(1), 18-38. https://he02.tci-thaijo.org/index.php/Veridian-E-Journal/article/view/31074/30063

Ebert, N., Ackermann, K. A., & Scheppler, B. (2021). Bolder is better: Raising user awareness through salient and concise privacy notices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-12). arXiv. https://arxiv.org/abs/2101.08021

Forbes. (2023). *10 marketing trends that will dominate in 2024.* https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2023/12/18/10-marketing-trends-that-will-dominate-in-2024/?sh=40b16d623586

Forrester. (2022). *Privacy isn't binary: The 2021 US privacy segmentation*. https://www.forrester.com/blogs/privacy-isnt-binary-the-2021-us-privacy-segmentation/

Gerber, N., Stöver, A., & Marky, K. (2023). *Human factors in privacy research.* Springer Nature.

Gupta, R., Iyengar, R., Sharma, M., Cannuscio, C. C., Merchant, R. M., Asch, D. A., Mitra, N., & Grande, D. (2023). Consumer views on privacy protections and sharing

of personal digital health information. *JAMA Network Open, 6*(2), 1-13. https://doi.org/10.1001/jamanetworkopen.2023.1305

Hoofnagle, C. J., & Urban, J. M. (2014). Alan Westin's privacy homo economicus. *Wake Forest Law Review, 49*, 261-317. https://ssrn.com/abstract=2434800

Knijnenburg, B. P., Page, X., Wisniewski, P., Lipford, H. R., Proferes, N., & Romano, J. (2022). *Modern socio-technical perspectives on privacy*. Springer Nature.

Kotler, P., Kartajaya, H., & Setiawan, I. (2021). *Marketing 5.0: Technology for humanity*. Nation Books.

Kulwanichchaiyanan, A. (2023). *Road to data-driven organizations*. An Intelligence.

Law and Development Research Center. (2020). *Thailand data protection guidelines 3.0: Guidelines on the protection of personal data*. Chulalongkorn University Printing House.

Leszczynska, M., & Baltag, D. (2024). Can I have it non-personalized? An empirical investigation of consumer willingness to share data for personalized services and ads. *Journal of Consumer Policy, 47*, 345-372. https://doi.org/10.1007/s10603-024-09568-9

Liu, W., Xu, K., & Yao, M. Z. (2023). Can you tell me about yourself? The impacts of chatbot names and communication contexts on users' willingness to self-disclose information in human–machine conversations. *Communication Research Reports, 40*(3), 122-133. https://doi.org/10.1080/08824096.2023.2212899

Morton, A., & Sasse, M. A. (2014). Desperately seeking assurances: Segmenting users by their information-seeking preferences. In *Proceedings of the 2014 Twelfth Annual International Conference on Privacy, Security and Trust* (pp. 102-111). IEEE. https://doi.org/10.1109/PST.2014.6890929

NECTEC. (2023). *Thailand service robot market and industry report 2022, with trends for 2023–2024*. https://www.nectec.or.th/wp-content/uploads/2023/03/NECTEC-Service-Robot_20230316-Full-Paper.pdf

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent-popups and demonstrating their influence. In *Proceedings of the 2020 CHI conference on human factors in computing systems* (pp. 1-13). arXiv. https://arxiv.org/abs/2001.02479

Osazuwa, C. M. (2024). Confidentiality, integrity, and availability in network systems: A review of related literature. *International Journal of Innovative Science and Research Technology, 8*(12), 1946-1955. https://doi.org/10.5281/ZENODO.10464076

OWASP. (2021). *OWASP Top 10 privacy risks version 2.0*. https://owasp.org/www-project-top-10-privacy-risks/

Panda Security. (2023). *15 Tips to Protect Personal Information Online for 2023*. https://www. pandasecurity.com/en/mediacenter/protect-personal-information/

Pattanavijit, E. (2015). Factors driving personal information disclosure: The case of Facebook single sign-on. *Journal of Information System in Business, 3*(2), 58-73. https://doi.org/10.14456/jisb.2017.11

Pimrabiab, P. (2020). *Relationships between merchant characteristics and willingness to disclose personal data: mediating role of perceived online privacy risk*. [Master's thesis, Chulalongkorn University]. Chula Digital Collections. https://digital.car.chula.ac.th/chulaetd/4209/

Ramasoota, P. & Panichpapiboon, S. (2013). Online privacy in Thailand: Public and strategic awareness. *Journal of Communication Arts, 31*(1), 131-150. https://so02.tci-thaijo.org/index.php/jcomm/article/view/213488/148500

Rojananark, D., Meechaisue, P., Piriyakul, M., & Chinuntdej, N. (2021). The effects of price value and privacy concern on the behavioral intention to use wristbands for health in controlling the relationship with personal innovativeness and coupon proneness and the effects of behavioral intention to use and willingness to pay and provide personal information. *Ph.D. in Social Sciences Journal, 11*(3), 649-664. https://doi.org/10.14456/phdssj.2021.48

Rosário, A. T., & Dias, J. C. (2023). How has data-driven marketing evolved: Challenges and opportunities with emerging technologies. *International Journal of Information Management Data Insights, 3*(2), 1-14. https://doi.org/10.1016/j.jjimei.2023.100203

Sangeen, M., Bhatti, N. A., Kifayat, K., Alsadhan, A. A., & Wang, H. (2023). Blind-trust: Raising awareness of the dangers of using unsecured public Wi-Fi networks. *Computer Communications. 209*, 359-367. https://doi.org/10.1016/j.comcom.2023.07.011

Schomakers, E. M., Lidynia, C., & Ziefle, M. (2019). A typology of online privacy personalities: Exploring and segmenting users' diverse privacy attitudes and behaviors. *Journal of Grid Computing, 17*(4), 727-747. https://doi.org/10.1007/s10723-019-09500-3

Songja, R. & Cheyjunya, P. (2024). Factor analysis of privacy personality and willingness to personal data disclosure: Consumer segmentation by online data privacy and marketing technology. In *Proceedings of the 8th National Communications Academic Conference 2024* (pp. 600-614). Chulalongkorn University, Thailand.

Sung, E. C., Bae, S., Han, D.-I. D., & Kwon, O. (2021). Consumer engagement via interactive artificial intelligence and mixed reality. *International Journal of Information Management, 60*, 102382. https://doi.org/10.1016/j.ijinfomgt.2021.102382

Syrmoudis, E. (2024). Unlocking personal data from online services: User studies on transparency practices. *Journal of Information Technology, 39*(1), 23-41. https://doi.org/10.1080/07370024.2024.2325347

TechTalkThai. (2023). *Salesforce survey reveals 91% of Thai consumers want to know if they're communicating with AI or a human when using services*. https://www.techtalkthai.com/salesforce-survey-reveals-91-of-thai-consumers-want-to-know-if-theyre-communicating-with-ai-or-humans-when-using-services/

Thanyarattakul, T. (2019). *Digital transformation in action: Transforming business in the digital age step by step*. Wish Publishing.

TrustArc. (2024). *Privacy in augmented and virtual reality platforms: Challenges and solutions*. https://trustarc.com/resource/privacy-augmented-virtual-reality-platforms/

Wutthiphaphinyo. N. (2021). *A study of factors affecting chatbot user's satisfaction* [Master' thematic paper, Mahidol University]. CMMU Digital Archive. https://archive.cm.mahidol.ac.th/handle/123456789/4123

Wuttidittachotti, P., Janloy, K., & Kittongpul, S. (2021). *Cyber security: Don't let anyone use your data*. Amarin How-To Amarin Printing and Publishing.