



UNVEILING CONSUMER RESISTANCE TO AUTOMATED DELIVERY ROBOT SERVICES: AN INFORMATION PRIVACY PERSPECTIVE

REVELANDO A RESISTÊNCIA DO CONSUMIDOR AOS SERVIÇOS DE ROBÔS DE ENTREGA AUTOMATIZADOS: UMA PERSPECTIVA DE PRIVACIDADE DA INFORMAÇÃO

XIANWEI LYU

UCSI Graduate Business School, UCSI University, Kuala Lumpur, Malaysia School of Digital Business and Intelligent Logistics, Jiangsu Vocational College of Business, Jiangsu, China.
Email: lyuxianwei6688@gmail.com

ABSTRACT

Objective: To explore the factors influencing consumer resistance to Automated Delivery Robots (ADRs) in delivery services, focusing on the impact of privacy concerns within the framework of the Antecedent-Privacy Concern-Outcome (APCO) model.

Methods: This study uses a mixed-method approach, including a survey with 416 valid responses and the combined importance-performance map analysis (cIPMA) method for data analysis. The research model examines the relationship between perceived vulnerabilities (technological, provider, legal) and privacy concerns, and how these relate to consumer resistance behaviors.

Results: The results indicate that technological, provider, and legal vulnerabilities significantly impact privacy concerns, which in turn, increase resistance behavior towards ADRs. Moreover, perceived autonomy and anthropomorphism were found to mitigate resistance, while the need for human interaction significantly moderated these relationships.

Conclusion: The findings suggest that while ADRs have potential in delivery services, their adoption is hindered by significant privacy concerns and vulnerabilities. Addressing these concerns through better privacy protections and enhancing user control can reduce consumer resistance and facilitate the adoption of ADR technologies.

Keywords: Autonomous delivery robots; Perceived vulnerability; Resistance behavior; Antecedent-privacy concern-outcome model; cIPMA





RESUMO

Objetivo: Explorar os fatores que influenciam a resistência do consumidor aos Robôs de Entrega Automatizados (ADRs) em serviços de entrega, focando no impacto das preocupações com a privacidade dentro do modelo Antecedente-Preocupação com a Privacidade-Resultado (APCO).

Métodos: Este estudo utiliza uma abordagem mista, incluindo uma pesquisa com 416 respostas válidas e o método de análise de mapa de importância-desempenho combinada (cIPMA) para análise de dados. O modelo de pesquisa examina a relação entre vulnerabilidades percebidas (tecnológica, de provedor, legal) e preocupações com a privacidade, e como estas se relacionam com comportamentos de resistência do consumidor.

Resultados: Os resultados indicam que as vulnerabilidades tecnológica, de provedor e legal impactam significativamente as preocupações com a privacidade, que por sua vez, aumentam o comportamento de resistência aos ADRs. Além disso, descobriu-se que a autonomia percebida e o antropomorfismo mitigavam a resistência, enquanto a necessidade de interação humana moderava significativamente essas relações.

Conclusão: Os achados sugerem que, embora os ADRs tenham potencial em serviços de entrega, sua adoção é impedida por preocupações significativas com a privacidade e vulnerabilidades. Abordar essas preocupações por meio de melhores proteções de privacidade e aprimoramento do controle do usuário pode reduzir a resistência do consumidor e facilitar a adoção de tecnologias ADR.

Palavras-chave: Robôs de entrega autônomos; Vulnerabilidade percebida; Comportamento de resistência; Modelo de preocupação com privacidade-resultado antecedente; cIPMA





1 INTRODUCTION

In the context of the current digital and information age, technological innovation has fully penetrated into many areas of daily life. The pace of integrating intelligent service robots into society is accelerating, and it is no longer a distant vision (Koh & Yuen, 2024). Automated robots have gradually shown their practical application value in various business operations, covering a wide range of fields such as the hotel industry, catering industry, and last-mile delivery (Lim et al., 2024; Wu et al., 2023). These robots can replace humans in completing household chores, item delivery and other related service tasks, significantly improving operational efficiency and service quality.

ADRs refer to robotic devices that utilize technologies such as artificial intelligence, automation, and sensors, enabling autonomous navigation and operation specifically for package and item delivery tasks (Srinivas et al., 2022). These robots are typically equipped with GPS, cameras, and other sensors, allowing them to perform precise localization and path planning in complex environments, thereby achieving efficient delivery services (Srinivas et al., 2022). Currently, prominent international logistics companies, such as FedEx (United States) and DHL (Germany), have established themselves as leaders in the field of autonomous delivery for package delivery services (Sham et al., 2023). In China, major retailers like Alibaba and JD.com have also made substantial investments in this domain. According to the Koh & Yuen (2023a), the ADR market is expected to rise significantly by 2029, becoming a key component in the global autonomous last-mile delivery sector, with an estimated market value of US\$211.3 million, highlighting the broad application prospects of ADR delivery services.

Despite the significant potential of ADRs and the generally positive attitude of most users toward their delivery services, there are still certain concerns expressed regarding the application of this innovative technology in the logistics and delivery industry (Said et al., 2023). According to Ayyildiz & Erdogan (2024), ADRs collect and store personal data during the delivery service process, which can be vulnerable to data breaches and hacker attacks, thereby posing a risk to user privacy and security. This is not surprising, as ADR delivery services are still a nascent practice undergoing phased testing and refinement. If ADR service providers fail to effectively ensure the security of users' private information, it is inevitable that users will question and resist the adoption of this innovative service, ultimately hindering its widespread





dissemination. In view of this, it is imperative to conduct a thorough exploration of potential users' concerns and expectations regarding privacy security, from their perspective. By doing so, logistics and delivery service providers will be able to tailor strategies that address the resistance encountered during the future implementation and promotion of ADR delivery services.

In the modern logistics industry, while the effective application of AI technology has significantly enhanced the efficiency of customer data processing, it has also inadvertently introduced potential risks of privacy data breaches among users (Soumpeniotti & Panagopoulos, 2023). As suggested by Quach et al. (2022), there is a compelling need for more extensive investigation into how emerging technologies (e.g., ADR) potentially pose threats to user information and privacy. Zhang & Zhang (2024) emphasized that the perceived vulnerabilities of emerging innovations services serve as a significant precursor to users' privacy concerns, which subsequently lead to resistance behaviors among users. Furthermore, in the context of intelligent robot services, Aw et al. (2023) suggested that combining the attributes of AI, such as autonomy and anthropomorphism, with other relevant and closely related structural elements, and incorporating them into the research framework, is expected to yield more insightful research outcomes.

While privacy challenges significantly impact the acceptance of emerging technological services (Aw et al., 2023; Lee, 2020; Ribeiro et al., 2024; Zhang & Zhang, 2024), a detailed examination of the specific factors influencing user privacy concerns and the mechanisms by which these factors lead to resistance towards adopting ADR services remains inadequately explored in the specific context of ADR delivery services. This study combines perceived vulnerabilities of ADR delivery services (covering technical, service provider, and legal aspects) with technological attribute factors (including autonomy and anthropomorphic characteristics), and innovatively incorporates these factors into the APCO model. This not only expands the application scope of the APCO model but also enhances its theoretical depth in explaining the acceptance of emerging technologies, further enriching the existing literature. Furthermore, logistics companies and policymakers can formulate more targeted guidelines and regulatory measures based on this, balancing the relationship between technological innovation and public privacy protection. This is expected to reduce users' resistance due to privacy concerns and promote the efficient promotion and user acceptance of this innovative service.

The research study has five sections. The introductory section provides the





study background; Section 2 covers the formulation of the theoretical framework and hypotheses. The research methodology is showed in Section 3, and the research findings are presented and discussed in Section 4. Finally, Section 5 discusses the conclusions and their implications.

2. THEORETICAL BACKGROUND AND HYPOTHESES DEVELOPMENT

2.1. Theoretical framework

The APCO framework is a comprehensive theoretical and empirical model that seeks to thoroughly capture and understand the factors that lead to privacy concerns and the resulting impact on consumer behavior (Alashoor et al., 2017; Smith et al., 2011). The essence of the framework is in its three distinct dimensions: antecedents, privacy concerns, and outcomes, which collectively constitute a methodical analytical framework. Depending on the specific context in which it is applied, different factors can be selected and measured within each of these dimensions to provide a nuanced understanding of privacy-related issues and their implications (Smith et al., 2011). Furthermore, the APCO model has been extensively utilized in various technological contexts, including home IoT services (Lee, 2020), face recognition payment systems (X. Zhang & Zhang, 2024), tracking applications (Duan & Deng, 2022), and more, actively engaging in topics pertaining to privacy. It has proven to be remarkably versatile and applicable when it comes to handling privacy problems. Expanding on this basis, this study cites the APCO model as a theoretical framework to align the variables being examined.

Vulnerability, a concept commonly defined as an individual's premonition or suspicion of impending potential harm (Smith & Cooper-Martin, 1997; Zhang & Zhang, 2024). Within the broad field of Information and Communication Technology (ICT), Khidzir et al. (2010) conducted a comprehensive and in-depth exploration of vulnerability as perceived by individuals. After systematic analysis and research, they successfully identified 30 significant vulnerability risk factors, which were further subdivided into four core categories: technology vulnerability, which is mainly related to system design flaws and weaknesses; provider vulnerability, which is associated with service reliability and vendor accountability mechanisms; legal vulnerability, which refers to the poor enforcement of relevant laws and regulations; and user vulnerability, which arises mainly from the ignorance and negligence of users themselves. In





addition, researches have shown that innovative services face multiple serious challenges in the diffusion and application phases, such as technological vulnerability, service provider vulnerability, legal vulnerability, and user vulnerability, which are not only significant, but also raise deep privacy concerns among users, whose seriousness cannot be ignored (Lee, 2020; X. Zhang & Zhang, 2024). As an innovation in the last-mile delivery service model, ADRs are gradually being promoted and applied in the logistics market (Lim et al., 2024). Therefore, this research also incorporates vulnerability assessments to examine users' privacy concerns and behavioral resistance towards the innovative delivery services provided by ADRs. It is worth noting that since user vulnerability involves more user-related factors rather than situational factors directly related to delivery services, it is excluded from the scope of this study.

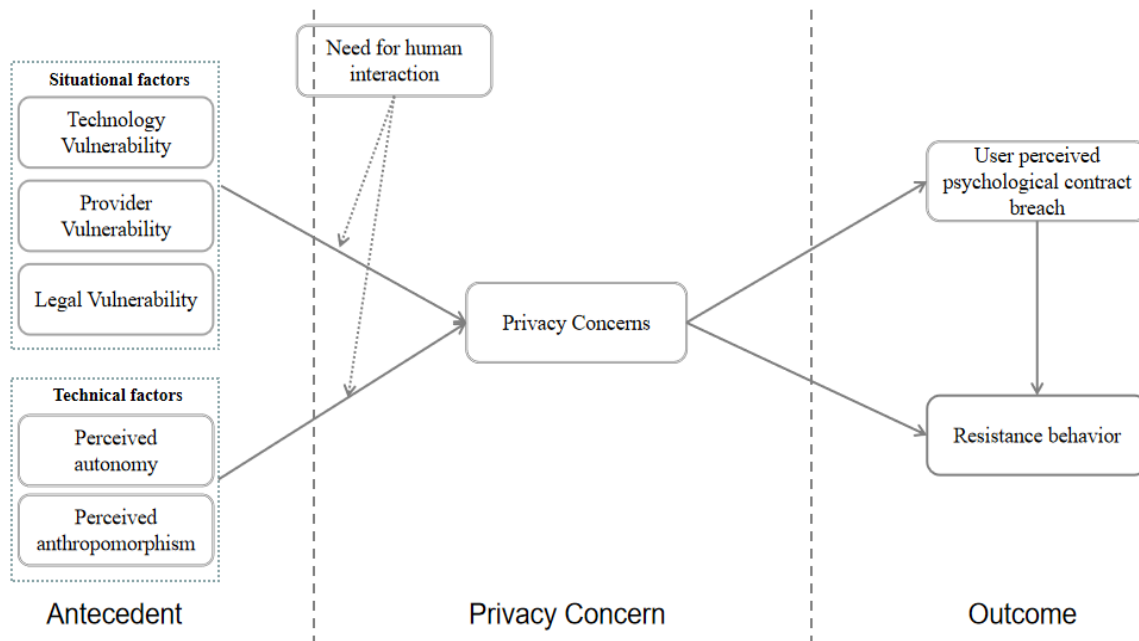
Building on previous research that advocates for an integrative theoretical approach (Sham et al., 2023), this study incorporates the CASA paradigm to support our extended investigation into human-like attributes. Specifically, we argue that anthropomorphism and autonomy of ADRs are prerequisites for privacy concerns in delivery services. The CASA theory indicates that users exhibit social reactions and responses to computers similar to those they show towards other humans (Reeves & Nass, 1996). In other words, individuals unconsciously apply the same social rules and heuristics used in interpersonal interactions when engaging with computers and other emerging technologies (Aw et al., 2023). Furthermore, the CASA theory has been widely applied and has become a significant theoretical framework for explaining human interactions and psychological responses to advanced technologies (e.g., social robot, autonomous vehicles) (Jin, 2023; Koh & Yuen, 2023b). In the context of last-mile delivery services, ADRs with anthropomorphic and autonomous features can make independent decisions and complete delivery tasks with minimal human intervention (Lim et al., 2024). This capability allows them to freely collect and process data in various environments, which may lead users to feel a loss of control over their personal information, thereby exacerbating privacy concerns.

2.2. Hypotheses development

Building on aforementioned ideas, Fig. 1 displays a conceptual framework for analyzing users' resistance to ADR delivery services from the perspective of privacy concerns. The research hypotheses are summarized below.



Fig. 1. Conceptual model.



2.2.1. Technology vulnerability

The technology vulnerability denotes the inherent weaknesses within technology systems, architectures, or applications, arising from deficiencies or flaws in their design and implementation processes (H. Lee, 2020). It reflects the instability and susceptibility to attacks that technology may exhibit when facing external threats, internal failures, or environmental changes. The deployment of last-mile ADRs has introduced significant advancements in logistics and consumer convenience (Koh & Yuen, 2023a). However, these technological innovations come with inherent vulnerabilities that pose substantial risks to user privacy. For instance, ADRs collect and transmit large amounts of user data during their operation, including addresses, purchase records, and personal preferences. Due to the early development stage of ADR systems and the vulnerabilities in internet security, hackers can potentially exploit these technical weaknesses to obtain sensitive information, leading to data breaches. In modern society, with the increasing frequency of cybersecurity incidents, users are becoming more aware of the need to protect their personal privacy (Mamonov & Benbunan-Fich, 2018). Frequent technical failures in ADR systems are bound to raise concerns among users about the safety of their privacy. Additionally, Lee (2020) highlighted a positive association between technology vulnerability and privacy concerns in the context of emerging technologies (e.g., Home Internet of Things

services). Given the preceding discussion, we propose the following hypothesis:

H1. Technology vulnerability positively and significantly influences user's privacy concerns.

2.2.2. Provider vulnerability

Provider vulnerability refers to the shortcoming that a service provider may fail to adequately manage or protect users' personal information, potentially prioritizing their own interests over the security and privacy of their clients (H. Lee, 2020). This shortcoming can lead to unauthorized access to personal data, misuse of sensitive information, and data breaches (H. Lee, 2020; Tang et al., 2008). In the realm of last-mile delivery services, ADR service providers bear the significant responsibility of handling vast datasets of user information. Given the sensitivity and privacy of user data, service providers must adopt stringent measures to maintain data security and integrity (King & Raja, 2012). However, if ADR delivery service providers fail to adequately fulfill this responsibility or sell user information for personal gain, it may inevitably lead to a severe loss of user trust and exacerbate public concerns about privacy breaches. Furthermore, Zhang & Zhang (2024) empirically demonstrated that provider vulnerability is significantly linked to privacy concerns in the context of facial recognition payment (FRP) adoption in China, and highlighting it play a crucial role in shaping the level of privacy concerns among users. We propose the following hypotheses in light of the preceding discussion:

H2. Provider vulnerability positively and significantly influences user's privacy concerns.

2.2.3. Legal vulnerability

Legal vulnerability denotes the deficiencies and shortcomings of current legal frameworks in effectively safeguarding personal privacy (Lee, 2020). The widespread application of big data technology has made the collection, storage, and analysis of personal data more frequent and efficient (Hashem et al., 2015). Despite users' ongoing concerns about data processing through information technology, the fragility of the privacy legal framework remains a significant issue that cannot be overlooked (Brookman, 2015). The root of this problem lies in the fact that the pace of legal reform has not kept pace with the rapid advancements in technology (Lee, 2020).

Consequently, the existing personal information protection laws face difficulties in adequately safeguarding personal information and user privacy in emerging technological environments, such as ADR delivery services. When personal privacy is violated, the lack of regulatory mechanisms often poses a significant obstacle to implementing appropriate punishment for infringing behaviors. Furthermore, in some instances, delaying the implementation of regulatory measures to facilitate the growth of emerging technology industries may inadvertently create legal loopholes, exacerbating concerns about personal privacy (H. Lee, 2020). In studies related to emerging technological services, evidence has shown that legal vulnerability notably impacts on users' privacy concerns (H. Lee, 2020; X. Zhang & Zhang, 2024). Specifically, the inadequacies in legal protection exacerbate users' worries about personal privacy security. Given the preceding discussion, we propose the following hypothesis:

H3. Legal vulnerability positively and significantly influences user's privacy concerns.

2.2.4. Perceived autonomy

In intelligent service robotics, autonomy refers to the ability of ADRs to operate independently (Huang et al., 2023). It is a key metric for evaluating the extent to which a technological entity can make and execute decisions without human intervention (Novak & Hoffman, 2019). The CASA theory emphasizes that interactions between humans and computers follow social rules and norms similar to those in interpersonal interactions (Reeves & Nass, 1996). In the context of ADR delivery services, users tend to perceive robots with autonomy as entities possessing social attributes rather than as mere tools or devices. Consequently, the autonomy of robots enhances their social credibility and sense of responsibility, leading users to trust their privacy protection measures more. Furthermore, Zhang et al. (2022) posited that service robots exhibit a superior performance to humans in the execution of routine tasks. Thus, the high autonomy of ADRs represents a reduction in human operation and intervention during the delivery process, reducing the risk of privacy breaches caused by human error. In the context of robo-advisory services, Aw et al. (2023) revealed that perceived autonomy positively impacts perceived justice, which in turn negatively influences privacy concerns. We propose the following hypotheses in light of the preceding discussion:

H4. Perceived autonomy negatively and significantly influences user's privacy

concerns.

2.2.5. Perceived anthropomorphism

Within the context of this study, anthropomorphism refers to the consumers' perception of the degree to which ADRs resemble humans in terms of appearance, behavior, and interaction style (Aw et al., 2023). Although anthropomorphism is generally regarded as a crucial element in customer interactions with robotic services, research findings on its effects on consumer behavior and psychological responses are significantly varied and inconsistent (Chuah et al., 2021). For instance, Li et al. (2024) conformed that users' acceptance of drone delivery services is positively and strongly associated with perceived anthropomorphic characteristics, thus shaping behavioral intentions. Another study suggested that perceived anthropomorphism can make consumers feel uncomfortable and feel that their human identity is being violated (Blut et al., 2021). Based on the CASA theory, when users perceive ADRs as entities with social behavior capabilities, they interact with them based on the principles of trust and reciprocity found in human interactions. This socialized interaction mode may make users more willing to trust that the robots will handle their personal information properly, thereby reducing privacy concerns. Additionally, anthropomorphic design features can reduce the negative impacts of intrusive technology on users' feelings of privacy invasion (Benlian et al., 2019). In the context of artificial intelligence services, Lee & Chen (2022) showed that perceived anthropomorphism significantly promotes trust, which is important for mitigating privacy concerns when disclosing personal information online (Bansal et al., 2016). Therefore, we propose the following hypotheses in light of the preceding discussion:

H5. Perceived anthropomorphism negatively and significantly influences user's privacy concerns.

2.2.6. Privacy concerns

Privacy concerns are a multifaceted and complex concept, deeply reflecting individuals' apprehensions about the potential infringement of their privacy rights due to personal information leaks (Dinev & Hart, 2006). It also encompasses their anxiety over losing control of sensitive information (Rath & Kumar, 2021). Such concerns are often closely linked with the adoption of new technologies, particularly in the context of

the widespread use of emerging technologies like intelligent service robots (Koh et al., 2023). Notably, users' privacy concerns significantly influence their decision-making behaviors (Yao et al., 2024). Psychological contract is based on the implicit or explicit expectations and commitments between the user and the service provider (Mason & Simmons, 2012). When users believe that the service provider has failed to act according to the mutually agreed rules or standards, they perceive a breach of the psychological contract (Lin et al., 2018). Trust is an important component of the psychological contract (Mehta et al., 2024), and when users have concerns about privacy protection, such concerns erode their trust in the service provider (K.-W. Wu et al., 2012), which in turn makes them more likely to perceive a breach of the psychological contract. Furthermore, empirical research findings showed that consumers' privacy concerns regarding emerging technology services are positively associated with their resistance behaviors (Aw et al., 2023; Liu et al., 2021; Zhang & Zhang, 2024). In light of the preceding discussion, we cautiously propose the following hypotheses:

H6a. Privacy concerns positively and significantly influence user perceived psychological contract breach.

H6b. Privacy concerns positively and significantly influence behavior resistance.

2.2.7. User perceived psychological contract breach

User perceived psychological contract breach, as a profound and complex subjective experience (Rousseau, 1998), refers in this study specifically to the user's perception that the service provider has failed to adequately fulfill the obligations promised within the psychological contract in the context of using automated delivery robot services (Lin et al., 2018). Based on social contract theory, an implicit contractual relationship exists between individuals and society or organizations, predicated on shared interests and mutual expectations (Culiberg, 2023). This relationship is equally relevant in the context of ADR delivery services, where users anticipate that service providers will uphold their promises to secure personal information privacy. Nonetheless, when a psychological contract breach occurs—indicating that the service provider has not fully honored their commitments—it may result in user resistance and potentially destructive behaviors. In addition, a study on information system implementation showed that there was a significant positive correlation between users' perceived psychological contract breach and resistance behavior (Lin et al., 2018). Cai

& Mardani (2023) highlighted that psychological contract breaches can trigger consumer resistance intentions in the context of personalized marketing. In light of the preceding discussion, we cautiously propose the following hypotheses:

H7. user perceived psychological contract breach positively and significantly influences behavior resistance.

2.2.8 The moderating effect of need for human interaction.

In this study, the need for human interaction refers to the degree to which users desire human contact during the delivery service experience with ADRs (Dabholkar, 1996). It profoundly reflects the users' inherent preference for human interaction when experiencing services and is considered a user characteristic that significantly impacts the modes and effectiveness of technological interactions (Dabholkar & Bagozzi, 2002). In the context of emerging technologies, extant literature has consistently demonstrated that the need for interpersonal interaction exerts both direct and indirect influences on users' psychological states and behavioral patterns (Chen et al., 2018; Song et al., 2022; Taufik & Hanafiah, 2019). Users with a higher need for human interaction often exhibit greater vigilance towards the potential vulnerabilities of emerging technologies and are more inclined to rely on human interaction to ensure safety and reliability in their service experiences (Xu et al., 2023), indicating that they are conservative about adopting new technologies or services and recognize the role of human interaction in reducing uncertainty and risk. This phenomenon is particularly prominent in the practical scenario of last-mile delivery services. Users with a higher need for human interaction show heightened alertness to the vulnerabilities of ADR services, such as technology vulnerability, service provider vulnerability, and legal vulnerability. Moreover, these users are more sensitive to the potential disturbances and concerns regarding privacy and security safeguards that these vulnerabilities may entail. In light of the preceding discussion, we cautiously propose the following hypotheses:

H8. Need for human interaction moderates the relationship between perceived vulnerability (i.e., (H8a) technology vulnerability; (H8b) provider vulnerability; (H8c) legal vulnerability) and privacy concerns, meaning that a higher level of need for human interaction results in a stronger positive relationship.

According to Dabholkar & Bagozzi (2002), users who prefer human interaction often lack the inherent motivation to adopt technology as a substitute for frontline

employees. They require a greater perception of technological advantages before accepting such changes. In other words, users with a high need for human interaction are more sensitive to improvements in the humanization of ADR services. They will accept the innovation and replacement of traditional services if the experience of using ADRs increasingly resembles their preferred traditional service experience. The autonomy and anthropomorphic attributes of robots significantly enhance the humanization and realism of the service experience (Li et al., 2022). Autonomy endows the robots with the ability to think and make decisions independently, enabling them to adapt flexibly in diverse service scenarios (Huang et al., 2023). The anthropomorphic design makes their interaction more human-like, improving their attentiveness and naturalness in the service process (Chuah et al., 2021). Therefore, users with a high need for human interaction are more likely to view ADR delivery services as being as attentive to privacy protection as traditional human services, thus alleviating privacy concerns. In light of the preceding discussion, we cautiously propose the following hypotheses:

H9. Need for human interaction moderates the relationship between robot technical factors (i.e., (H9a) perceived autonomy, (H9b) perceived anthropomorphism) and privacy concerns, meaning that a higher level of need for human interaction results in a stronger negative relationship.

3. METHODOLOGY

3.1 Data collection and sample

This study employed a purposive sampling strategy, targeting Chinese users who have not yet used ADR delivery services. The aim was to thoroughly investigate the factors influencing their resistance to such services. To achieve this, we conducted an online survey using the specialized Chinese survey platform “WJX” (<http://www.wjx.cn>) and successfully collected 508 responses. The data underwent a rigorous screening process, including attention checks, the removal of duplicate responses, and an evaluation of the time taken to complete the survey questionnaires. After these data cleaning steps, 416 complete and valid questionnaires were retained for further analysis. Additionally, the sample size obtained in this study exceeded the minimum sample size requirement of 112, as calculated using G*Power software. Furthermore, the gender distribution among the respondents was relatively balanced,

with females accounting for 53.1% and males for 46.9%. Notably, approximately half of the respondents were aged between 26 and 34, an age group that coincides with those most concerned about privacy issues (Kezer et al., 2016). Lastly, the vast majority of respondents held a bachelor's degree.

3.2. Measures

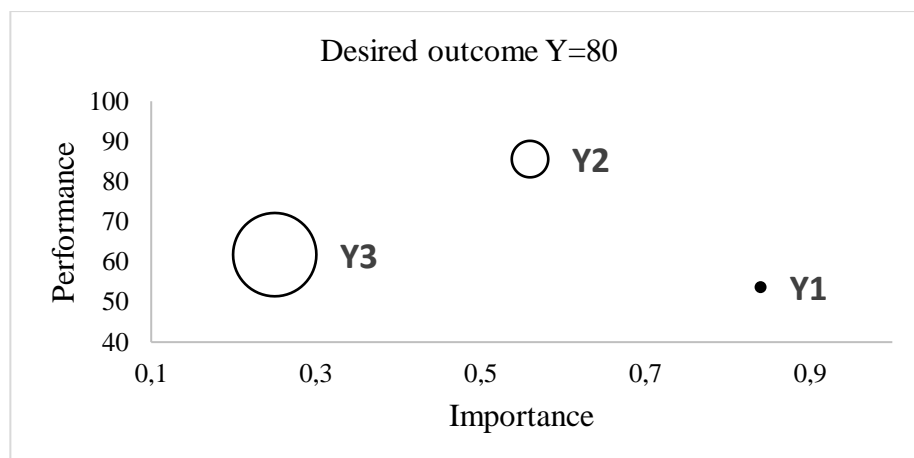
To align the previously validated questionnaire scales with the specific context of the current research, the scales were slightly modified and adapted for this study. As depicted in Appendix A, each primary construct comprises several secondary items. All items were measured using a 7-point Likert scale, where 1 indicates strong disagreement, and 7 indicates strong agreement. Additionally, this study rigorously implemented two stages: a pre-test, involving four academic experts and three industry experts, and a pilot test, involving 46 respondents. These steps were taken to further ensure the validity and reliability of the data collection process.

3.3 Data analysis

This study follows the recommendations of Hauff et al. (2024) and adopts the Combined importance–performance map analysis (cIPMA) method, using SmartPLS4 software for data analysis. This approach integrates the results of Necessary Condition Analysis (NCA) into Partial Least Squares Structural Equation Modeling (PLS-SEM), thereby extending and deepening the traditional Importance-Performance Map Analysis (IPMA) (Hauff et al., 2024). When conducting data analysis using the cIPMA (Hauff et al., 2024), the initial step involves executing the IPMA to evaluate the importance and performance of each antecedent construct relative to the target construct. The quantification of importance is achieved by calculating the total effect of each construct on the target construct, while performance is measured based on the average rescaled construct score. Subsequently, a NCA is performed, with the aim of determining the conditions that must be met to achieve a specific level of the target construct. A condition is considered necessary if it simultaneously satisfies predetermined criteria for the p-value and effect size (d), specifically requiring a p-value less than 0.05 and an effect size d greater than 0.1 (Dul, 2016). Finally, the results from the PLS-SEM, IPMA, and NCA are integrated to construct a comprehensive map that clearly illustrates the importance, performance, and necessity of each antecedent

construct, providing a holistic perspective and deep insights into the data analysis (See Fig. 2). Furthermore, the cIPMA method has been successfully applied using SmartPLS 4 software in the extended version of Davis's (1989) Technology Acceptance Model (TAM) (Hauff et al., 2024; Sarstedt et al., 2024).

Fig. 2. cIPMA of the TAM



Note: For the desired level of the outcome: • = construct is not necessary; ○ = construct is necessary. The bubble sizes represent the percentage of cases that have not achieved the required desired level outcome.

4. RESULTS

4.1. Common method bias (CMB)

To ensure that CMB is mitigated, this study followed the recommendations of Podsakoff et al. (2003) by implementing both procedural and statistical remedies. Procedurally, we ensured that each question in the questionnaire was clearly and unambiguously phrased. Additionally, data collection was conducted at different times, across various locations, and in diverse environments. We also strictly maintained the anonymity of respondents and the confidentiality of the data throughout the survey process. Regarding statistical remedies, the CMB was evaluated by performing Harman's single-factor test (Podsakoff et al., 2003). The outcome indicated that the single factor accounted for 33.641% of the variance, which is below the threshold of 50%. Furthermore, in accordance with the method for assessing full collinearity recommended by Kock (2015), the variance inflation factors (VIF) for all constructs ranged from 1.000 to 1.960, which were all below the threshold of 3.30. From the

above, it is clear that CMB is not an essential problem.

4.2. Measurement model assessment

As indicated in Table 1, the minimum values of Cronbach's Alpha and Composite reliability are 0.809 and 0.884, respectively, both exceeding the threshold of 0.7 set for establishing reliability (Aw et al., 2023). Concurrently, the minimum values of the Average Variance Extracted (AVE) and the outer loadings also reach 0.655 and 0.768, jointly satisfying the threshold conditions of being higher than 0.5 and 0.7 (Hair et al., 2019), respectively, required for establishing convergent validity. Furthermore, the findings (Table 2) show that the maximum value of Heterotrait-Monotrait (HTMT) is 0.622, which meets the recommended threshold of being less than 0.85 (Aw et al., 2023). Additionally, the Fornell-Larcker criterion indicates that the diagonal elements representing the square root of AVE are more significant than the correlation coefficients of the variables, thus demonstrating that discriminant validity is also met. Lastly, we examined the outer weights of all indicators, and the results showed that all outer weights are positive.

Table 1- Quality criteria.

Construct	Indicators	Weights	Loadings	Alpha	CR	AVE
TEV	TEV1	0.382	0.885	0.845	0.906	0.763
	TEV2	0.410	0.871			
	TEV3	0.353	0.865			
PRV	PRV1	0.369	0.810	0.809	0.887	0.723
	PRV2	0.353	0.851			
	PRV3	0.451	0.888			
LEV	LEV1	0.372	0.883	0.850	0.909	0.770
	LEV2	0.367	0.849			
	LEV3	0.401	0.900			
PAU	PAU1	0.270	0.768	0.824	0.884	0.655
	PAU2	0.334	0.856			
	PAU3	0.324	0.788			
	PAU4	0.305	0.824			
PAN	PAN1	0.290	0.920	0.914	0.940	0.796
	PAN2	0.282	0.892			
	PAN3	0.273	0.889			
	PAN4	0.277	0.865			
PRC	PRC1	0.167	0.804	0.924	0.939	0.689
	PRC2	0.169	0.793			
	PRC3	0.182	0.858			
	PRC4	0.18	0.870			
	PRC5	0.181	0.855			
	PRC6	0.155	0.806			
	PRC7	0.170	0.818			
NHI	NHI1	0.306	0.894	0.890	0.924	0.752

Construct	Indicators	Weights	Loadings	Alpha	CR	AVE
	NHI2	0.243	0.829			
	NHI3	0.283	0.862			
	NHI4	0.318	0.882			
PCB	PCB1	0.399	0.895	0.840	0.904	0.758
	PCB2	0.349	0.834			
	PCB3	0.399	0.881			
REB	REB1	0.409	0.887	0.834	0.900	0.750
	REB2	0.324	0.819			
	REB3	0.418	0.890			

Notes: TEV =Technology Vulnerability; PRV=Provider Vulnerability; LEV=Legal Vulnerability; PAU=Perceived Autonomy; PAN=Perceived Anthropomorphism; PRC=Privacy concerns; NHI=Need for human interaction; PCB=User perceived psychological contract breach; REB=Resistance Behavior.

Table 2- Discriminant validity (HTMT).

	LEV	NHI	PAN	PAU	PCB	PRC	PRV	REB	TEV
LEV									
NHI	0.448								
PAN	0.533	0.416							
PAU	0.467	0.290	0.451						
PCB	0.462	0.461	0.433	0.327					
PRC	0.573	0.472	0.522	0.542	0.622				
PRV	0.248	0.137	0.427	0.420	0.261	0.405			
REB	0.296	0.294	0.344	0.078	0.598	0.490	0.111		
TEV	0.461	0.325	0.447	0.542	0.409	0.487	0.382	0.216	

4.3. Structural model assessment

After comprehensively evaluating the measurement model, this study proceeded to assess the structural model. The coefficients of determination (R^2) for privacy concerns, user perceived psychological contract breach, and resistance behavior are 0.491, 0.303 and 0.291, respectively, all exceeding the 0.26 threshold established by Cohen (1988), indicating sufficient explanatory power. Additionally, the Q^2 values for all endogenous variables are greater than zero, suggesting that the model possesses reasonable predictive relevance (Hair et al., 2011). To further evaluate the predictive performance of the study model, we adopted the PLSpredict method as suggested by Hair et al. (2019). According to the data presented in Table 3, the PLS model demonstrates lower root mean square error (RMSE) values for most indicators compared to the linear regression model. This result indicates that our study model exhibits moderate predictive ability.

Table 3- PLS-predict assessment.

Items	Q ² predict	PLS-SEM_RMSE	LM_RMSE
PCB1	0.190	1.458	1.466
PCB2	0.160	1.458	1.468
PCB3	0.198	1.384	1.415
PRC1	0.282	1.352	1.398
PRC2	0.284	1.335	1.367
PRC3	0.348	1.273	1.336
PRC4	0.338	1.307	1.325
PRC5	0.361	1.349	1.394
PRC6	0.228	1.355	1.388
PRC7	0.245	1.378	1.412
REB1	0.068	1.620	1.632
REB2	0.039	1.389	1.407
REB3	0.082	1.433	1.469

Table 4 presents the analysis results for all hypotheses. Specifically, technology vulnerability ($\beta=0.134$, $p<0.01$), provider vulnerability ($\beta=0.155$, $p<0.001$), and legal vulnerability ($\beta=0.260$, $p<0.001$) are all significantly positively correlated with privacy concerns (H1, H2, and H3). Conversely, perceived autonomy ($\beta=-0.220$, $p<0.001$) displays a significant negative correlation with privacy concerns (H4). However, the hypothesized negative correlation between perceived anthropomorphism ($\beta=-0.097$, $p>0.05$) and privacy concerns is not supported (H5). Furthermore, privacy concerns ($\beta=0.550$, $p<0.001$) exhibit a significant positive correlation with users perceived psychological contract breach (H6a). Both privacy concerns ($\beta=0.226$, $p<0.001$) and users perceived psychological contract breach ($\beta=0.381$, $p<0.001$) show a significant positive correlation with resistance behavior (H6b and H7).

In the analysis of moderating relationships, need for human interaction significantly moderates the positive correlation between technology vulnerability ($\beta=0.132$, $p<0.05$), legal vulnerability ($\beta=0.155$, $p<0.01$) and privacy concerns, but does not moderate the relationship between provider vulnerability ($\beta=0.044$, $p>0.05$) and privacy concerns. Therefore, H8a and H8c are supported, while H8b is not. Additionally, need for human interaction significantly moderates the negative correlation between perceived autonomy and privacy concerns ($\beta=0.132$, $p<0.05$), but does not moderate the relationship between perceived anthropomorphism and privacy concerns ($\beta=0.027$, $p>0.05$). Hence, H9a is supported, while H9b is not.

Table 4- Results of hypotheses testing.

Hypotheses Relationship	Std. Beta	t-value	p-value	Support?
H1 TEV -> PRC	0.134	3.026	0.001	YES
H2 PRV -> PRC	0.155	3.568	0	YES
H3 LEV -> PRC	0.260	6.148	0	YES
H4 PAU -> PRC	-0.220	3.979	0	YES
H5 PAN -> PRC	-0.097	1.411	0.079	NO
H6a PRC -> PCB	0.550	10.171	0	YES
H6b PRC -> REB	0.226	3.426	0	YES
H7 PCB -> REB	0.381	6.029	0	YES
H8a NHI x TEV -> PRC	0.132	2.246	0.012	YES
H8b NHI x PRV -> PRC	0.044	0.748	0.227	NO
H8c NHI x LEV -> PRC	0.155	2.948	0.002	YES
H9a NHI x PAU -> PRC	0.132	1.889	0.030	YES
H9b NHI x PAN -> PRC	0.027	0.443	0.329	NO

4.4. cIPMA

IPMA enables a thorough assessment of the antecedents of the target construct in terms of both importance (i.e., Total Effect) and performance (i.e., Latent Variable Score), and provides valuable insights for optimizing the target construct accordingly (Ringle & Sarstedt, 2016). Referring to the results of IPMA as shown in Table 5 and Fig. 3, among the antecedents of the target structure of REB, the order of importance from high to low is PRC (0.435), PCB (0.381), LEV (0.118), TEV (0.055), PRV (0.053), PAN (-0.079) and PAU (-0.086); the order of performance scores from high to low is PRV (68.524), PCB (67.890), PRC (67.416), LEV (64.753), TEV (60.819), PAN (54.503) and PAU (51.703).

Subsequently, we extracted the rescaled latent variable scores from IPMA and entered them into the NCA (Hauff et al., 2024). The statistical significance and effect sizes (d) of the latent construct are ascertained and examined with a 5000-random sample size, as Sarstedt et al. (2024) advised. The d and p-values for each antecedent structure of REB are shown in Table 6. The results showed that TEV, PRV, LEV and PCB are significant necessary conditions ($d > 0.1$, $p < 0.05$) for REB. It is noteworthy that, given the d values of PAU, PAN, and PRC are all less than the threshold of 0.1 (Dul, 2016), these three variables are excluded from the potential antecedents constituting the necessary conditions for REB. Furthermore, we set the number of steps for the bottleneck table to 20, aiming to identify the minimum bottleneck percentage conditions

required for all antecedent structures to fail to meet the expectation level of REB (See Table 7). As can be seen from Table 7, 25% of all cases did not achieve the necessary level of TEV to enable the expectation 85% level of REB. In other words, at this level of expectation, 75 % of TEV cases resulted in REB. By analogy, the percentages of other antecedents leading to the expectation 85% level of REB are as follows: PRV at 89.183%, LEV at 84.375% and PCB at 94.952%.

Table 5 - IPMA results.

Latent Variables	Performance	Importance
TEV	60.819	0.055
PRV	68.524	0.053
LEV	64.753	0.118
PAU	51.703	-0.086
PAN	54.503	-0.079
PRC	67.416	0.435
PCB	67.890	0.381

Fig. 3. IPMA for REB.

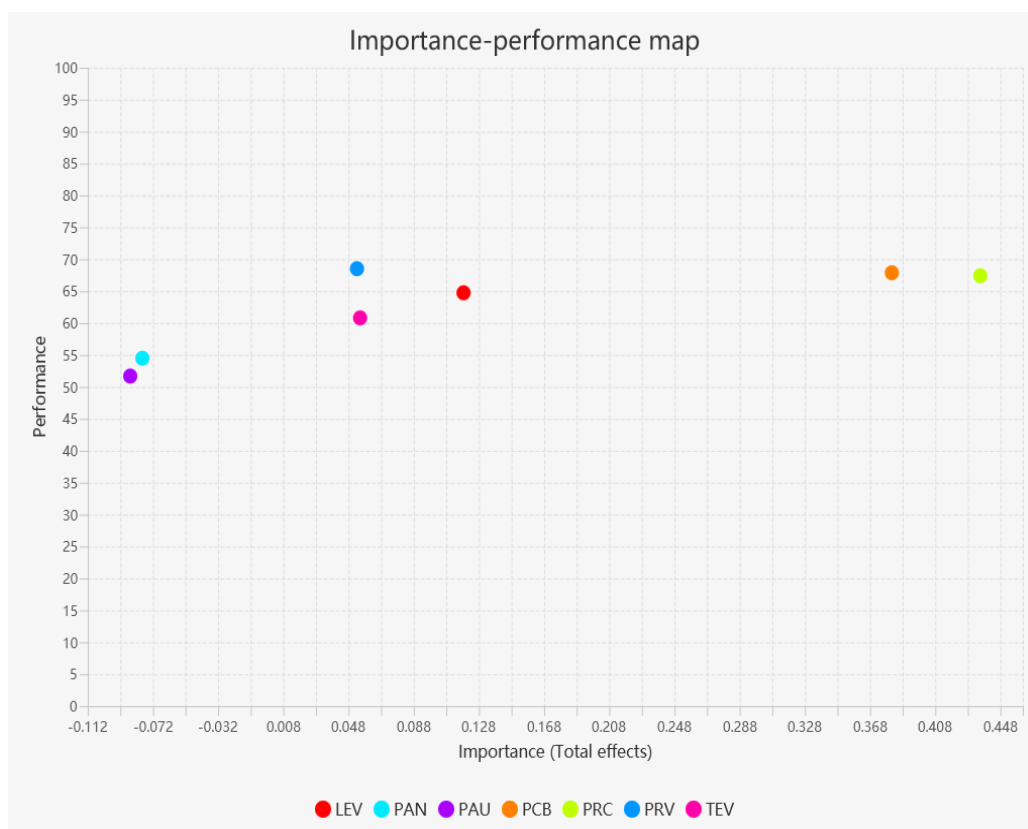


Table 6- NCA effect sizes and P-value

Construct	Effect size d	P-value
TEV	0.162	0
PRV	0.114	0
LEV	0.130	0
PAU	0.048	0.15
PAN	0	0
PRC	0.095	0
PCB	0.129	0

Table 7- Percentage of bottlenecks that do not reach the expected level of REB.

	TEV	PRV	LEV	PAU	PAN	PRC	PCB
0.00%	NN	NN	NN	NN	NN	NN	NN
5.00%	NN	NN	NN	NN	NN	NN	NN
10.00%	NN	NN	NN	NN	NN	NN	NN
15.00%	NN	NN	NN	NN	NN	NN	NN
20.00%	NN	NN	NN	NN	NN	NN	NN
25.00%	NN	NN	NN	0.240	NN	NN	NN
30.00%	NN	NN	NN	0.481	NN	NN	NN
35.00%	NN	NN	NN	0.481	NN	0.240	NN
40.00%	NN	NN	NN	0.481	NN	0.240	NN
45.00%	0.24	NN	NN	0.481	NN	3.125	NN
50.00%	0.24	NN	NN	0.481	NN	3.125	NN
55.00%	1.202	NN	NN	0.481	NN	3.125	NN
60.00%	1.202	NN	NN	0.481	NN	3.125	1.683
65.00%	1.442	NN	3.125	0.962	NN	4.087	5.048
70.00%	5.769	0.240	5.769	0.962	NN	4.567	5.048
75.00%	9.615	1.683	15.625	0.962	NN	4.567	5.048
80.00%	18.750	10.817	15.625	0.962	NN	4.567	5.048
85.00%	25.000	10.817	15.625	0.962	NN	4.567	5.048
90.00%	27.163	16.827	33.173	0.962	NN	4.567	5.048
95.00%	48.317	83.413	38.221	0.962	NN	48.798	92.788
100.00%	48.317	83.413	38.221	0.962	NN	48.798	92.788

Note: NN = not necessary.

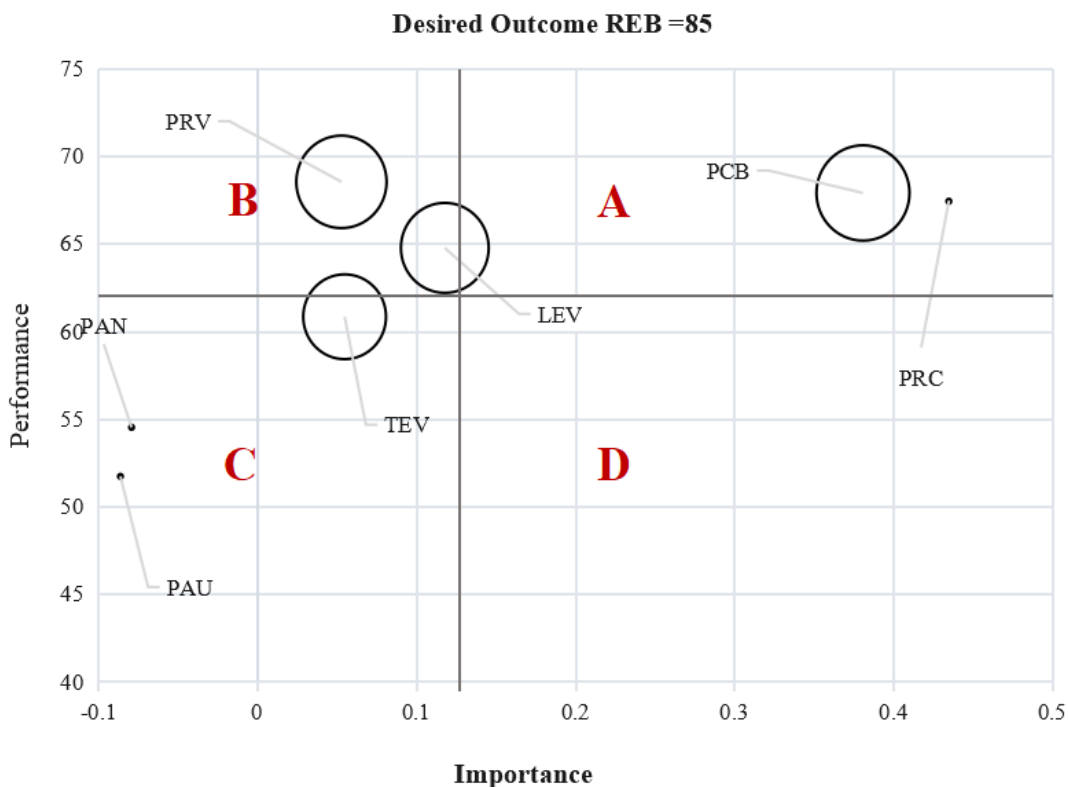
Lastly, we aggregated the data results from Table 5.6.7 and consolidated them into Table 8, upon which we constructed the combined importance-performance map for REB (See Fig.4). Meanwhile, we calculated the average importance of the existing variables, which yielded a mean importance of 0.125. Similarly, the average performance resulted in a mean performance of 62.230. Utilizing these mean importance and mean performance values, we divided the map in Figure 4 into four quadrants (A, B, C, and D). In this map, (1) the horizontal axis represents the importance score, (2) the vertical axis represents the performance score, and (3) the type of circle is used to indicate the necessity of the antecedent construct (where the white circle represents 'necessary' and the black circle represents 'non-necessary'). (4) Given that the aim of this study is to identify the influencing factors of resistance

behavior and further optimize and mitigate such behavior based on these factors, we used the size of the white circles to visually represent the percentage of cases corresponding to each antecedent construct that achieves the desired level of resistance behavior. The results presented in Figure 4 indicate that both PCB and PRC are located in Quadrant A, with PCB being identified as the sole necessary condition. In contrast, PRV and LEV belong to Quadrant B, and both are considered necessary conditions. TEV, PAN, and PAU are classified in Quadrant C, with TEV being the only one recognized as a necessary condition.

Table 8 -cIPMA results for REB

Antecedent construct	Performance	Importance	Percentage of bottlenecks met at 85% of the desired level.	Effect size d (P-value)	Necessary condition?
TEV	60.819	0.055	75.000	0.162 (0)	YES
PRV	68.524	0.053	89.183	0.114 (0)	YES
LEV	64.753	0.118	84.375	0.130 (0)	YES
PAU	51.703	-0.086	/	0.048 (0.15)	NO
PAN	54.503	-0.079	/	0 (0)	NO
PRC	67.416	0.435	/	0.095 (0)	NO
PCB	67.890	0.381	94.952	0.129 (0)	YES

Fig. 4. Combined importance-performance map of REB.



5. DISCUSSION AND CONCLUSIONS

5.1. Discussion of the results

Based on the evaluation results of PLS-SEM, Hypotheses 1, 2, and 3 are all supported, indicating a positive correlation between technology vulnerability, provider vulnerability, legal vulnerability, and privacy concerns. These findings further validate and confirm the finding of Zhang & Zhang (2024) on the positive impact of perceived vulnerability on privacy concerns in the context of facial recognition payment technology services. The autonomy attribute of ADRs is negatively correlated with privacy concerns, supporting Hypothesis 4, and aligning with the findings of Aw et al. (2023) that the autonomy of robo-advisors indirectly negatively affects privacy concerns through perceived justice. However, Hypothesis 5, which suggests that anthropomorphism has a negative impact on privacy concerns, was not supported. In response to this phenomenon, Blut et al. (2021) proposed a potential explanation based on the Uncanny Valley theory. They suggested that if an AI robot possesses an excessively high level of anthropomorphism, it may elicit feelings of unease and fear among users. Consequently, anthropomorphism does not alleviate concerns about privacy. Furthermore, the finding of this study provide evidence for Hypothesis 6a, demonstrated that privacy concerns positively influence user perceived psychological contract breach. According to Li & Slee's (2014), higher privacy concerns reflect users' higher expectations and demands for personal information protection. As a result, when businesses fail to meet these expectations, users are more prone to perceiving a breach of the psychological contract. Hypothesis 6b, which posits that privacy concerns positively influence resistance behavior, is also supported. This finding is consistent with the research conducted by Prakash & Das (2022) on digital contact tracing applications, as well as the investigation by Liu et al. (2021) regarding facial recognition payment technologies. The results of this study empirically support Hypothesis 7, indicating a positive correlation between user perceived psychological contract breach and resistance behavior. This finding is consistent with the conclusions drawn by Lin et al. (2018) in their research on user resistance behavior towards information system providers.

In terms of the analysis of moderating relationships, the data analysis results support Hypotheses H8a and H8c. Specifically, the need for human interaction



positively moderates the positive correlation between technology vulnerability and privacy concerns, as well as the positive correlation between legal vulnerability and privacy concerns. The reason for this finding may be that the need for human interaction reflects user's preference for human-to-human interaction when accessing services, rather than interaction with machines (Priya & Sharma, 2023). This preference indicates users' distrust in the technological aspect of innovative services and their legal protection, which subsequently exacerbates their concerns about privacy issues. However, Hypothesis H8b, which proposes that the need for human interaction positively moderates the positive correlation between provider vulnerability and privacy concerns, was rejected. This outcome may be attributed to the relatively limited scope of the need for human interaction, which makes it difficult to comprehensively cover all aspects of service provider management. In addition, in the hypotheses regarding the moderating effect of the need for human interaction on the relationship between autonomy and anthropomorphism with privacy concerns, H9a is supported, while H9b is rejected. Specifically, as stated in the study by Aw et al. (2023), based on the CASA theory, the higher the level of autonomy exhibited by intelligent robots, the more they tend to mimic human behavior and follow social norms, thus paying more attention to privacy protection. Therefore, an increased need for human interaction further strengthens the negative correlation between autonomy and privacy concerns, meaning H9a is confirmed. Since the negative correlation between perceived anthropomorphism and privacy concerns was not confirmed (i.e., H3 was not supported), H9b was also not supported.

Based on the analysis results of cIPMA, we found that technology vulnerability, provider vulnerability, legal vulnerability, and user perceived psychological contract breach are significant necessary conditions for resistance behavior. Specifically, 75%, 89.183%, 84.375%, and 94.952% of the cases, respectively, met the 85% level required for resistance behavior. This finding further validates the related conclusions regarding resistance behavior in Lee (2020) study on home Internet of Things services, as well as in Klaus & Blanton (2010) research on enterprise system implementation. Given the high importance and performance level of users perceived psychological contract breach, it should be considered a key element for priority optimization. It is worth noting that privacy concerns are a primary antecedent of resistance behavior with the highest level of importance. However, privacy concerns are not a necessary condition for such behavior. This may be because not all users prioritize privacy protection, and there are various factors that can lead to user resistance to robotic





services, such as value barriers and communication barriers (Koh & Yuen, 2024). Lastly, perceived autonomy and perceived anthropomorphism effectively alleviate resistance behavior, indirectly confirming that autonomy and anthropomorphism enhance users' acceptance of intelligent robot services (Li & Wang, 2022).

5.1 Theoretical implications

As an important and innovative technology in the logistics industry, ADRs are likely to encounter both adoption and resistance from users during their introduction and promotion. As highlighted by Aw et al. (2023), resistance to innovation is considered one of the key factors that prevent new products and services from successfully entering the market. Gaining a deep understanding of user resistance to emerging products and services is crucial for ensuring their promotion, long-term development, and sustainability. Building on this foundation, this study draws on the recommendations of previous research (Zhang & Zhang, 2024) and to propose and validate a research framework with a privacy perspective. The mechanisms of users' privacy concerns about ADR delivery services are clarified and further analyzed how these privacy concerns affect users' behaviour outcomes, contributing to the literature in the field of ADRs.

Moreover, this study extends the autonomy and anthropomorphic attributes of ADRs into the APCO framework. Previous research has primarily focused on the impact of autonomy and anthropomorphism attributes on the acceptance of service robots (Aw, Zha, et al., 2023; Li & Wang, 2022), yet there has been scant exploration of how these two factors interact with privacy concerns. Our research not only provides practical insights for overcoming the inherent limitations of the APCO model but also broadens the research horizon of ADRs by proposing an innovative framework that considers the interplay between autonomy, anthropomorphism and privacy concerns in the field of service robots.

In the field of research on privacy concerns of emerging technological services, the main focus is usually on the vulnerability of the technology or service, and user perceptions (Liu et al., 2021; X. Zhang & Zhang, 2024). However, this study reveals an important yet often overlooked dimension: users' need for human interaction. Specifically, when users place a high value on human interaction, they may be more inclined to remain connected to traditional service models as a way of maintaining their personal privacy space. In view of this, this study takes the need for human interaction



as a key moderating variable to explore the intrinsic links between vulnerability, robot attributes and privacy concerns in a more nuanced way, providing new perspectives and insights into the study of privacy concerns in this area.

5.2 Practical implications

This study provides several practical applications for ADR service providers and policymakers. Firstly, it reveals that users perceived psychological contract breach is an important antecedent and a necessary condition for resistance behavior. Therefore, enterprises should prioritize and strive to maintain psychological contracts with users, ensuring that the introduction of ADR services does not violate users' basic expectations regarding service experience, data security, and privacy protection. By adopting transparent communication strategies, clear service commitments, and effective privacy protection measures, enterprises can reduce the risk of users perceived psychological contract breach, thereby mitigating the occurrence of resistance behavior. On the other hand, although privacy concerns constitute a major precursor to users' resistance towards ADR services, they are not a necessary condition for such resistance. Therefore, in the process of advancing ADR services, enterprises should not confine themselves solely to refining privacy protection strategies, but should instead adopt a more comprehensive and holistic approach. This includes optimizing and enhancing technical vulnerabilities, provider vulnerabilities, and legal vulnerabilities, with the aim of comprehensively reducing users' willingness to resist. Lastly, in recognition that perceived autonomy and anthropomorphism effectively mitigate users' resistance, enterprises should prioritize enhancing the autonomous decision-making capabilities of ADRs and endow them with more human-like characteristics during the design and development process. This is done with the dual aims of protecting user privacy and enhancing service acceptance and market competitiveness.

6. LIMITATIONS AND FUTURE RESEARCH

Undoubtedly, this study has certain limitations. The first and foremost point to note is that the quantitative method of online surveys may inherently have limitations in comprehensively capturing the nuanced viewpoints and deep-seated feelings of users towards ADR delivery services. Given this consideration, future research can



adopt qualitative research methods, such as focus group discussions or in-depth interviews, to explore and understand users' comprehensive perspectives on ADR delivery services, as well as the underlying reasons and motivations behind them, in a more profound manner. Secondly, this study is limited to exploring the internal vulnerability factors inherent in the delivery services provided by ADRs, without considering the potential threats from external factors. In light of this, future research directions that combine internal vulnerabilities with external threat factors for deeper analysis are expected to more comprehensively reveal and understand users' resistance to the delivery services provided by ADRs and the underlying reasons behind it. Thirdly, although this study's model has explored privacy issues within the context of ADR services, there remains significant scope for further analysis from various dimensions, such as social and cultural perspectives. Given the diverse types of information involved in privacy breaches, each with distinct characteristics, developing a comprehensive model that thoroughly examines these sub-dimensions of privacy would greatly enhance our understanding of the broader privacy concerns. Lastly, the sample population of this study is confined to Chinese users. Given that cultural differences may lead to variations in consumers' cognition, beliefs, and values, further research is necessary to validate the applicability of this model to user groups in other countries, thereby ensuring its universal applicability and cross-cultural validity.

REFERENCES

Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO model. *Communications of the Association for Information Systems*, 41(1), 4.

Aw, E. C.-X., Leong, L.-Y., Hew, J.-J., Rana, N. P., Tan, T. M., & Jee, T.-W. (2023a). Counteracting dark sides of robo-advisors: Justice, privacy and intrusion considerations. *International Journal of Bank Marketing*. <https://doi.org/10.1108/IJBM-10-2022-0439>

Aw, E. C.-X., Leong, L.-Y., Hew, J.-J., Rana, N. P., Tan, T. M., & Jee, T.-W. (2023b). Counteracting dark sides of robo-advisors: Justice, privacy and intrusion considerations. *International Journal of Bank Marketing*, 42(1), 133–151. <https://doi.org/10.1108/IJBM-10-2022-0439>

Aw, E. C.-X., Zha, T., & Chuah, S. H.-W. (2023). My new financial companion! Non-linear understanding of Robo-advisory service acceptance. *The Service Industries Journal*, 43(3–4), 185–212. <https://doi.org/10.1080/02642069.2022.2161528>





- Ayyildiz, E., & Erdogan, M. (2024). Addressing the challenges of using autonomous robots for last-mile delivery. *Computers & Industrial Engineering*, 190, 110096. <https://doi.org/10.1016/j.cie.2024.110096>
- Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, 53(1), 1–21.
- Benlian, A., Klumpe, J., & Hinz, O. (2019). Mitigating the Intrusive Effects of Smart Home Assistants by using Anthropomorphic Design Features: A Multi-Method Investigation. *Information Systems Journal*, 30. <https://doi.org/10.1111/isj.12243>
- Blut, M., Wang, C., Wunderlich, N. V., & Brock, C. (2021). Understanding anthropomorphism in service provision: A meta-analysis of physical robots, chatbots, and other AI. *Journal of the Academy of Marketing Science*, 49(4), 632–658. <https://doi.org/10.1007/s11747-020-00762-y>
- Brookman, J. (2015). Protecting Privacy in an Era of Weakening Regulation. *Harvard Law & Policy Review*, 9, 355.
- Cai, H., & Mardani, A. (2023). Research on the impact of consumer privacy and intelligent personalization technology on purchase resistance. *Journal of Business Research*, 161, 113811. <https://doi.org/10.1016/j.jbusres.2023.113811>
- Chen, Y., Yu, J., Yang, S., & Wei, J. (2018). Consumer's intention to use self-service parcel delivery service in online retailing: An empirical study. *Internet Research*, 28(2), 500–519. <https://doi.org/10.1108/IntR-11-2016-0334>
- Chuah, S. H.-W., Aw, E. C.-X., & Yee, D. (2021). Unveiling the complexity of consumers' intention to use service robots: An fsQCA approach. *Computers in Human Behavior*, 123, 106870. <https://doi.org/10.1016/j.chb.2021.106870>
- Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences* (2nd ed.). Routledge. <https://doi.org/10.4324/9780203771587>
- Culiberg, B. (2023). Psychological contract breach and opportunism in the sharing economy: Examining the platform-provider relationship. *Industrial Marketing Management*.
- Dabholkar, P. A. (1996). Consumer evaluations of new technology-based self-service options: An investigation of alternative models of service quality. *International Journal of Research in Marketing*, 13(1), 29–51. [https://doi.org/10.1016/0167-8116\(95\)00027-5](https://doi.org/10.1016/0167-8116(95)00027-5)
- Dabholkar, P. A., & Bagozzi, R. P. (2002). An attitudinal model of technology-based self-service: Moderating effects of consumer traits and situational factors. *Journal of the Academy of Marketing Science*, 30, 184–201.
- Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), 319–340. <https://doi.org/10.2307/249008>





- Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>
- Duan, S. X., & Deng, H. (2022). Exploring privacy paradox in contact tracing apps adoption. *Internet Research*, 32(5), 1725–1750. <https://doi.org/10.1108/INTR-03-2021-0160>
- Dul, J. (2016). Necessary Condition Analysis (NCA): Logic and Methodology of “Necessary but Not Sufficient” Causality. *Organizational Research Methods*, 19(1), 10–52. <https://doi.org/10.1177/1094428115584005>
- Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice*, 19(2), 139–152. <https://doi.org/10.2753/MTP1069-6679190202>
- Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, 31(1), 2–24. <https://doi.org/10.1108/EBR-11-2018-0203>
- Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of “big data” on cloud computing: Review and open research issues. *Information Systems*, 47, 98–115.
- Hauff, S., Richter, N. F., Sarstedt, M., & Ringle, C. M. (2024). Importance and performance in PLS-SEM and NCA: Introducing the combined importance-performance map analysis (cIPMA). *Journal of Retailing and Consumer Services*, 78, 103723. <https://doi.org/10.1016/j.jretconser.2024.103723>
- Huang, D., Chen, Q., Huang, S. (Sam), & Liu, X. (2023). Consumer intention to use service robots: A cognitive–affective–conative framework. *International Journal of Contemporary Hospitality Management*, ahead-of-print(ahead-of-print). <https://doi.org/10.1108/IJCHM-12-2022-1528>
- Jin, S. V. (2023). “To comply or to react, that is the question:” the roles of humanness versus eeriness of AI-powered virtual influencers, loneliness, and threats to human identities in AI-driven digital transformation. *Computers in Human Behavior: Artificial Humans*, 1(2), 100011. <https://doi.org/10.1016/j.chbah.2023.100011>
- Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(1). <https://cyberpsychology.eu/article/view/6182>
- Khidzir, N. Z., Mohamed, A., & Arshad, N. H. (2010). Information security risk factors: Critical threats vulnerabilities in ICT outsourcing. *2010 International Conference on Information Retrieval & Knowledge Management (CAMP)*, 194–199. <https://doi.org/10.1109/INFRKM.2010.5466918>
- King, N. J., & Raja, V. T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review*, 28(3), 308–319. <https://doi.org/10.1016/j.clsr.2012.03.003>





Klaus, T., & Blanton, J. E. (2010). User resistance determinants and the psychological contract in enterprise system implementations. *European Journal of Information Systems*, 19(6), 625–636. <https://doi.org/10.1057/ejis.2010.39>

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of E-Collaboration (Ijec)*, 11(4), 1–10.

Koh, L. Y., Lee, J. Y., Wang, X., & Yuen, K. F. (2023). Urban drone adoption: Addressing technological, privacy and task–technology fit concerns. *Technology in Society*, 72, 102203. <https://doi.org/10.1016/j.techsoc.2023.102203>

Koh, L. Y., & Yuen, K. F. (2023a). Consumer adoption of autonomous delivery robots in cities: Implications on urban planning and design policies. *Cities*, 133, 104125. <https://doi.org/10.1016/j.cities.2022.104125>

Koh, L. Y., & Yuen, K. F. (2023b). Public acceptance of autonomous vehicles: Examining the joint influence of perceived vehicle performance and intelligent in-vehicle interaction quality. *Transportation Research Part A: Policy and Practice*, 178, 103864. <https://doi.org/10.1016/j.tra.2023.103864>

Koh, L. Y., & Yuen, K. F. (2024). The role of motivators, barriers, attractiveness, and positive emotions on consumers' intention to adopt and resist self-driving delivery robots. *Journal of Retailing and Consumer Services*, 81, 103998. <https://doi.org/10.1016/j.jretconser.2024.103998>

Lee, H. (2020). Home IoT resistance: Extended privacy and vulnerability perspective. *Telematics and Informatics*, 49, 101377. <https://doi.org/10.1016/j.tele.2020.101377>

Lee, J.-C., & Chen, X. (2022). Exploring users' adoption intentions in the evolution of artificial intelligence mobile banking applications: The intelligent and anthropomorphic perspectives. *International Journal of Bank Marketing*, 40(4), 631–658. <https://doi.org/10.1108/IJBM-08-2021-0394>

Li, T., & Slee, T. (2014). The effects of information privacy concerns on digitizing personal health records. *Journal of the Association for Information Science and Technology*, 65(8), 1541–1554. <https://doi.org/10.1002/asi.23068>

Li, X., Lee, G. J. X., & Yuen, K. F. (2024). Consumer acceptance of urban drone delivery: The role of perceived anthropomorphic characteristics. *Cities*, 148, 104867. <https://doi.org/10.1016/j.cities.2024.104867>

Li, Y., & Wang, C. (2022). Effect of customer's perception on service robot acceptance. *International Journal of Consumer Studies*, 46(4), 1241–1261. <https://doi.org/10.1111/ijcs.12755>

Li, Y., Wang, C., & Song, B. (2022). Customer acceptance of service robots under different service settings. *Journal of Service Theory and Practice*, 33(1), 46–71. <https://doi.org/10.1108/JSTP-06-2022-0127>

Lim, X.-J., Chang, J. Y.-S., Cheah, J.-H., Lim, W. M., Kraus, S., & Dabić, M. (2024). Out of the way, human! Understanding post-adoption of last-mile delivery robots. *Technological Forecasting and Social Change*, 201, 123242. <https://doi.org/10.1016/j.techfore.2024.123242>





Lin, T.-C., Huang, S.-L., & Chiang, S.-C. (2018). User resistance to the implementation of information systems: A psychological contract breach perspective. *Journal of the Association for Information Systems*, 19(4), 2.

Liu, Y., Yan, W., & Hu, B. (2021). Resistance to facial recognition payment in China: The influence of privacy-related factors. *Telecommunications Policy*, 45(5), 102155. <https://doi.org/10.1016/j.telpol.2021.102155>

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, 83, 32–44.

Mason, C., & Simmons, J. (2012). Are they being served? Linking consumer expectation, evaluation and commitment. *Journal of Services Marketing*, 26(4), 227–237. <https://doi.org/10.1108/08876041211237532>

Mehta, A., Mall, S., Kothari, T., & Deshpande, R. (2024). Hotel employees' intention to stay through psychological contract fulfillment and positive emotions in post-lockdown era. *Tourism Review*, 79(1), 104–118.

Novak, T. P., & Hoffman, D. L. (2019). Relationship journeys in the internet of things: A new framework for understanding interactions between consumers and smart objects. *Journal of the Academy of Marketing Science*, 47(2), 216–237. <https://doi.org/10.1007/s11747-018-0608-3>

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879.

Prakash, A. V., & Das, S. (2022). Explaining citizens' resistance to use digital contact tracing apps: A mixed-methods study. *International Journal of Information Management*, 63, 102468. <https://doi.org/10.1016/j.ijinfomgt.2021.102468>

Priya, B., & Sharma, V. (2023). Exploring users' adoption intentions of intelligent virtual assistants in financial services: An anthropomorphic perspectives and socio-psychological perspectives. *Computers in Human Behavior*, 148, 107912. <https://doi.org/10.1016/j.chb.2023.107912>

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, 50(6), 1299–1323. <https://doi.org/10.1007/s11747-022-00845-y>

Rath, D. K., & Kumar, A. (2021). Information privacy concern at individual, group, organization and societal level—A literature review. *Vilakshan - XIMB Journal of Management*, 18(2), 171–186. <https://doi.org/10.1108/XJM-08-2020-0096>

Reeves, B., & Nass, C. (1996). The media equation: How people treat computers, television, and new media like real people. *Cambridge, UK*, 10(10), 19–36.

Ribeiro, R., Neto, J. S., Orlandi, T. R. C., Orlandi, R. de A. L. (2024). A Tool for Privacu Culture Assessment. *International Journal of Behavior Studies in Organizations*, 11, 45-58. <https://doi.org/10.32038/JBSO.2024.12.04>





Ringle, C. M., & Sarstedt, M. (2016). Gain more insight from your PLS-SEM results: The importance-performance map analysis. *Industrial Management & Data Systems*, 116(9), 1865–1886.

Rousseau, D. M. (1998). The “Problem” of the Psychological Contract Considered. *Journal of Organizational Behavior*, 19, 665–671.

Said, M., Aeschliman, S., & Stathopoulos, A. (2023). Robots at your doorstep: Acceptance of near-future technologies for automated parcel delivery. *Scientific Reports*, 13(1), Article 1. <https://doi.org/10.1038/s41598-023-45371-1>

Sarstedt, M., Richter, N. F., Hauff, S., & Ringle, C. M. (2024). Combined importance–performance map analysis (cIPMA) in partial least squares structural equation modeling (PLS–SEM): A SmartPLS 4 tutorial. *Journal of Marketing Analytics*. <https://doi.org/10.1057/s41270-024-00325-y>

Sham, R., Chong, H. X., Cheng-Xi Aw, E., Bibi Tkm Thangal, T., & Abdamia, N. B. (2023). Switching up the delivery game: Understanding switching intention to retail drone delivery services. *Journal of Retailing and Consumer Services*, 75, 103478. <https://doi.org/10.1016/j.jretconser.2023.103478>

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

Smith, N. C., & Cooper-Martin, E. (1997). Ethics and Target Marketing: The Role of Product Harm and Consumer Vulnerability. *Journal of Marketing*, 61(3), 1–20. <https://doi.org/10.1177/002224299706100301>

Song, M., Xing, X., Duan, Y., Cohen, J., & Mou, J. (2022). Will artificial intelligence replace human customer service? The impact of communication quality and privacy risks on adoption intention. *Journal of Retailing and Consumer Services*, 66, 102900. <https://doi.org/10.1016/j.jretconser.2021.102900>

Soumpenioti, V., & Panagopoulos, A. (2023). AI Technology in the Field of Logistics. *2023 18th International Workshop on Semantic and Social Media Adaptation & Personalization (SMAP) 18th International Workshop on Semantic and Social Media Adaptation & Personalization (SMAP 2023)*, 1–6. <https://ieeexplore.ieee.org/abstract/document/10255203/>

Srinivas, S., Ramachandiran, S., & Rajendran, S. (2022). Autonomous robot-driven deliveries: A review of recent developments and future directions. *Transportation Research Part E: Logistics and Transportation Review*, 165, 102834. <https://doi.org/10.1016/j.tre.2022.102834>

Tang, Z., hu, Y. (Jeffrey), & smith, M. D. (2008). Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor. *Journal of Management Information Systems*, 24(4), 153–173. <https://doi.org/10.2753/MIS0742-1222240406>

Taufik, N., & Hanafiah, M. H. (2019). Airport passengers’ adoption behaviour towards self-check-in Kiosk Services: The roles of perceived ease of use, perceived usefulness and need for human interaction. *Heliyon*, 5(12). [https://www.cell.com/heliyon/fulltext/S2405-8440\(19\)36619-8](https://www.cell.com/heliyon/fulltext/S2405-8440(19)36619-8)





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

Wu, M., Tan, G. W.-H., Aw, E. C.-X., & Ooi, K.-B. (2023). Unlocking my heart: Fostering hotel brand love with service robots. *Journal of Hospitality and Tourism Management*, 57, 339–348. <https://doi.org/10.1016/j.jhtm.2023.10.014>

Xu, W., Dainoff, M. J., Ge, L., & Gao, Z. (2023). Transitioning to Human Interaction with AI Systems: New Challenges and Opportunities for HCI Professionals to Enable Human-Centered AI. *International Journal of Human-Computer Interaction*, 39(3), 494–518. <https://doi.org/10.1080/10447318.2022.2041900>

Yao, Q., Hu, C., & Zhou, W. (2024). The impact of customer privacy concerns on service robot adoption intentions: A credence/experience service typology perspective. *Technological Forecasting and Social Change*, 198, 122948. <https://doi.org/10.1016/j.techfore.2023.122948>

Zhang, S., Hu, Z., Li, X., & Ren, A. (2022). The impact of service principal (service robot vs. human staff) on service quality: The mediating role of service principal attribute. *Journal of Hospitality and Tourism Management*, 52, 170–183. <https://doi.org/10.1016/j.jhtm.2022.06.014>

Zhang, X., & Zhang, Z. (2024). Leaking my face via payment: Unveiling the influence of technology anxiety, vulnerabilities, and privacy concerns on user resistance to facial recognition payment. *Telecommunications Policy*, 48(3), 102703. <https://doi.org/10.1016/j.telpol.2023.102703>



Appendix A: Constructs and measurement items

Construct	Items	Adapted source
Technology Vulnerability (TEV)	<p>Devices for ADR delivery services would be vulnerable to external invasion.</p> <p>Transmission information may be leaked when using ADR delivery services.</p> <p>My personal information would not be technically secure when using ADR delivery services.</p>	(Lee, 2020)
Provider Vulnerability (PRV)	<p>ADR delivery service providers are not doing their duty to protect my personal information.</p> <p>ADR delivery service providers do not manage my personal information securely.</p> <p>ADR delivery service providers have not established appropriate privacy policies.</p>	(Lee, 2020)
Legal Vulnerability (LEV)	<p>There are problems in the privacy laws of my country to use ADR delivery services safely.</p> <p>Even if privacy is violated while using ADR delivery services, our legal system cannot protect me.</p> <p>Even if ADR delivery service provider infringes on privacy, they do not receive sufficient legal sanctions.</p>	(Lee, 2020)
Perceived Autonomy (PAU)	<p>The ADR determines how it conducts tasks by itself.</p> <p>The ADR makes decisions by itself.</p> <p>The ADR takes the initiative.</p> <p>The ADR does things by itself.</p>	(Aw et al., 2023)
Perceived Anthropomorphism (PAN)	<p>ADRs in the last-mile delivery services are natural; I do not feel fake about it.</p> <p>ADRs in the last-mile delivery services are humanlike.</p> <p>ADRs in the last-mile delivery services are conscious of their actions.</p> <p>ADRs in the last-mile delivery services are elegant in engaging.</p>	(Wu et al., 2023)
Privacy concerns (PRC)	<p>I am concerned about my privacy during the ADR delivery transaction.</p> <p>I am concerned that ADR delivery services would collect my personal information for other purposes without my consent.</p> <p>I am concerned that ADR delivery services would collect and share my personal information with third parties without my consent.</p> <p>I am concerned that too much of my personal information would be collected by ADR delivery services.</p> <p>I am concerned that ADR delivery services would collect my personal information and use it in a way I did not anticipate.</p> <p>I am concerned that my personal daily living activities would be monitored/captured by ADR delivery services.</p> <p>I am concerned that my residential location would be exposed through ADR delivery services.</p>	(Koh et al., 2023)
Need for human interaction (NHI)	<p>I enjoy the process of communicating with human service agent.</p> <p>Personalized response from human service is very important to me.</p> <p>I like communicating with human service agent.</p> <p>Interacting with automated delivery robot bothers me more than human service agent.</p>	(Song et al., 2022)
User perceived psychological	<p>My ADR delivery service provider has NOT done an excellent job of meeting its promises.</p>	(Lin et al., 2018)



contract breach (PCB)	My ADR delivery service provider did NOT come through in fulfilling the promises it made. My ADR delivery service provider has broken many of its promises on this delivery service project.
Resistance Behavior (REB)	I think I will not use ADR delivery services. (Lee, 2020) I will use more secure service than ADR delivery services. I will not recommend ADR delivery services to others.

