DECISION CRITERIA FOR EVALUATION OF CONSUMER PRIVACY AND SECURITY ASPECTS IN PLATFORM BUSINESS MODELS: A STUDY ON SRI LANKA PLATFORM BUSINESSES

Indra Mahakalanda
University of Moratuwa
Sri Lanka
indram@uom.lk

Ishari Siriwardena
Sri Lanka Telecom
ishari@slt.com.lk

ABSTRACT

In the evolving landscape of digital economies, platform business models—also known as digital business models—have emerged as dominant forces driving innovation, connectivity, and commerce. However, the pervasive integration of data within these platforms, data monetization, and intra/inter-firm benefit sharing have associated privacy-related costs for consumers. Thus, firm-consumer interactions have amplified concerns regarding privacy tensions among consumers, firms, and regulators. We explore the multifaceted criteria of privacy within digital platform business models, highlighting its critical importance. The objective of this article is to develop a Fuzzy Analytic Hierarchy Process (FAHP) for the evaluation of consumer privacy and security criteria of platform business models, taking into consideration the judgments of decision makers. First, it identifies six criteria and fourteen sub-criteria that constitute consumer privacy and security aspects in digital business models. The FAHP questionnaire survey collects data from industry experts and the FAHP assigns weights for each criterion, enabling decision makers the ability to rank them based on their importance level. This study only focuses on the main criteria for evaluation of consumer privacy and security in digital platforms. Results of the FAHP analysis rank the user awareness and education and compliance and regulatory framework criteria with the highest importance, while assigning the lowest weight to the data collection practices criterion. Our multi-criteria decision framework provides a comprehensive understanding of privacy's pivotal role in the success and sustainability of platform business models. Ultimately, this study contributes to the ongoing discourse on privacy, advocating for robust privacy strategies that balance innovation and ethical responsibility in the digital age.

Keywords: platform business models; consumer privacy and security; Multi-Criteria Decision Analysis; Analytical Hierarchy Process

1. Introduction

In the digital era, platform business models have transformed business operations, providing unparalleled prospects for expansion and innovation. As a result of extensive adoption of digital platform businesses, the notions of privacy have begun to evolve at a rapid pace (Tufekci, 2008). These models present considerable issues, especially regarding consumer privacy and security. As platforms accumulate and analyze extensive quantities of personal data, safeguarding this information has emerged as a vital issue for both enterprises and consumers. It is inevitable that different types of privacy tensions occur as a result of complex firm-consumer interactions (Quach et al., 2022).

According to Deloitte's "Connected Consumer" survey, 48% of respondents experienced at least one kind of security failure in the past year, up from 34% in 2023. Additionally, 85% of consumers have actively taken steps to protect themselves from such incidents. Only 22% believe platforms are transparent about how their data is used (Deloitte, 2024). Data protection authorities across Europe issued a total of EUR 1.64 billion in fines since January 2022, marking a 50% year-on-year increase (DLA Piper, 2023). The results are more acute in emerging markets, where 70% of consumers expressed concerns about how their data is being used by technology platforms. This has a significant impact on their trust and willingness to engage with new digital services (KPMG, 2024). Rising concerns over trust, privacy, and security among consumers can significantly impact platform business models (Lutz et al., 2018). As consumers become more cautious about how their data is used, platforms may experience reduced user engagement and slower adoption rates (Wang, 2020). This can lead to a decline in revenue and market share, as trust is a critical factor in consumer decision-making. Additionally, platforms may face increased regulatory scrutiny and higher compliance costs, further straining their resources. To mitigate these impacts, platform providers must prioritize robust data privacy measures, transparent practices, and effective communication to rebuild and maintain consumer trust (Nooren et al., 2018).

Consumer privacy pertains to the rights and expectations of individuals concerning the collection, utilization, and dissemination of their personal information. In platform business models, privacy issues are exacerbated by the massive data collection techniques adopted by these platforms. Security encompasses the strategies implemented to safeguard data against unwanted access, breaches, and various cyber threats.

Privacy focuses on the use and governance of personal data, while security is about the protection of data (Stalla-Bourdillon, 2014). As platform business models continue to evolve, addressing the critical criteria of consumer privacy and security is imperative. By understanding and mitigating the risks associated with data collection and usage, regulatory compliance, technological safeguards, and ethical considerations, platforms can build a sustainable and trustworthy digital ecosystem. In the context of platform businesses (e.g., ridesharing, e-commerce, food delivery), data privacy and security pose unique challenges that are not fully addressed by existing evaluation frameworks.

ISSN 1936-6744
https://doi.org/10.13033/ijahp.v18i1.1346

The objective of this article is to provide a comprehensive understanding of different criteria determining privacy and security aspects in a platform business model and their significance in terms of priority level that would support evaluating the success and sustainability of the platforms. This study contributes to the existing body of knowledge in the following two ways: development of a hierarchical structure for the evaluation criteria for consumer security and privacy and prioritization of main criteria using a Multi-Criteria Decision Analysis (MCDA) approach.

We used the Fuzzy Analytical Hierarchy Process (FAHP), a popular MCDA approach, to determine the relative importance of each dimension. Ultimately, this study contributes to the ongoing discourse on privacy, advocating for robust privacy strategies that balance innovation and ethical responsibility in the digital age. By establishing a comprehensive evaluation framework, managers can better identify and mitigate privacy risks, enhancing consumer trust and engagement. This proactive approach not only ensures regulatory compliance but also strengthens the platform's competitive advantage in a market increasingly concerned with data privacy and security. Unlike previous studies, this work introduces a fuzzy multi-criteria framework tailored to platform businesses, bridging the privacy-security gap with a novel application of the FAHP.

Despite the growing importance of privacy and security in platform business models, existing research often addresses these aspects in isolation, lacking a unified framework for comprehensive evaluation. To address this gap, the following literature review examines key dimensions of consumer privacy and security, focusing on both theoretical foundations and practical criteria relevant to digital platforms. This review establishes the basis for the criteria and framework developed in this study, ensuring that the subsequent model is grounded in established scholarship and tailored to the unique challenges faced by platform business models.

2. Literature review

This literature review encompasses the information privacy and security aspects of digital platform business models.

2.1 Digital platform business models

Rochet and Tirole (2003) define a digital platform as an interconnected marketplace that operates via the internet where buyers and sellers can exchange goods, services and information. Today, these new platform business models have an increasing strategic importance for firms.

Online platforms are the architects of digital transformation. These platforms provide consumers and sellers with various trade solutions. In addition to engaging in in-person transactions at stores, these platforms can also conduct exchanges in a virtual, impersonal, and ostensibly anonymous environment. The decrease in search costs, the enhancement of delivery speed, and the augmented market transparency represent the positive aspects of

this revolution. Nevertheless, these corporations also handle a substantial volume of customer data. Companies that operate as platform business models—such as Amazon, Apple, and Google—collect, process, organize, and disclose users' data to third parties for commercial and marketing purposes (Padilla et al., 2022). In the most adverse scenario, these platforms may act with illicit intentions. The data collected by platforms encompasses a wide array of individual information, including users' demographic data such as gender, age, and geographic location, as well as their browsing behaviors and previous transactions, and social engagement, among other factors. Consequently, platforms can predict users' preferences and behaviors and social tastes and capitalize on this information through targeted offers. Consumer data may potentially be misappropriated and utilized for illicit reasons, which would compromise consumers and their privacy (e.g., credit card and/or identity theft). This is considered one of the principal adverse aspects of the digital revolution (Dhirani et al., 2023).

2.2 Consumer privacy and security of online consumer information

The literature suggests approaches such as Westin's topology (Westin, 2000), Solove's taxonomy (Solove, 2006)) and privacy as a contextual integrity (Nissenbaum, 2004) to better understand different dimensions of privacy. The former is about privacy attitudes. Solove's taxonomy refers to collection, processing, dissemination and invasion of information. The latter refers to a conceptual framework for understanding privacy expectations and the related implications.

Internet-based platform business models lack borders and regulations, making privacy a top priority for online activity. Xu et al. (2008) explain information privacy as a multidimensional concept that depends on the context, individual's life experiences and the ability to control access to personal information. As a result, defining the concept of consumer privacy is challenging. Typically, consumer transactions generate personal information. Issues related to privacy are a result of collecting, processing, analyzing, using, storing and sharing this personal information (Chan et al., 2005) and also the methodologies adopted for processing information (Solove, 2006). Culnan (2000) points out that privacy of consumer information collected by commercial entities is a legal consumer right. On the other hand, from the economic point of view, privacy can be commoditized if it is a non-absolute right (Campbell & Carlson, 2002).

Most of the privacy literature refers to privacy and security as a single construct (Xu et al., 2008). Security concerns can be thought of as a dimension of privacy concerns. Gurung and Raja (2016) consider privacy and security concerns as a single construct of consumer intention to participate in e-commerce. However, counter arguments to this idea exist. For example, Vijayasarathy (2004) considers privacy and security as two different constructs. This study treats data privacy and security as interconnected facets of consumer trust in platforms—aligning with some of the previous studies (Xu et al., 2008)—thereby evaluating a holistic set of criteria. However, we recognize distinctions (privacy relates to data handling and consent, while security pertains to protection against breaches), and our framework incorporates both of these constructs for completeness.

Consumer concerns that include growing databases, personal data volume, privacy breaches, and data loss, mandates that platform companies implement tools and mechanisms to limit data collection, disclose the purpose of data collection, implement controls for data collection, restrict data access only for intended users, and use the data only for the intended purpose (Culnan, 1993; Hiller & Cohen, 2001). Online companies include privacy policies and disclaimers on their websites to enhance consumer trust. Online privacy policies aim to decrease consumer fear of privacy disclosure (Westin, 2000). Privacy rules mainly revolve around the country-specific privacy laws and governing regulatory conditions (Wu et al., 2012). However, for this research, we limit our discussion to the legal and regulatory landscape of privacy within the Sri Lankan context.

The Personal Data Protection Act (PDPA) enacted in Sri Lanka incorporates key principles of fair information practices, including notification, choice, access, security, and enforcement (Abeysekara & Ranasinghe, 2022). The principle of notification emphasizes that individuals must be informed about an entity's data-handling practices prior to the collection or use of personal information. Choice refers to providing individuals with options regarding how their personal data will be utilized. Access ensures that users can review their own data, verify its accuracy, and request corrections or updates. To maintain data integrity, organizations are required to implement measures that allow consumers to edit, update, or delete outdated information, or anonymize data where appropriate. Security mandates that personal data be safeguarded against unauthorized access or breaches. Finally, enforcement is essential to ensure compliance with these principles, supported by national and international guidelines on personal information management (Culnan, 1993; Hiller & Cohen, 2001).

Digital platforms frequently collect extensive personal information to personalize user experiences and inform business strategies. However, such practices raise concerns regarding transparency and the scope of data usage (Sargiotis, 2024). Compliance with data protection regulations, such as Sri Lanka's PDPA, is critical for mitigating legal risks and preserving consumer trust (Abeysekara & Ranasinghe, 2022). To safeguard user data, platforms must adopt advanced technological measures, including encryption, access controls, and data masking, to prevent breaches and unauthorized access (Cao et al., 2022). Beyond regulatory compliance, ethical considerations play a pivotal role in shaping responsible data practices. Platforms should foster a culture of trust and accountability, ensuring that consumer privacy is respected throughout all stages of data handling (Su & Jin, 2022).

Despite the increasing emphasis on consumer privacy and security within platform business models, a significant research gap persists in developing a comprehensive framework for evaluating these dimensions. Existing studies tend to address isolated aspects rather than adopting an integrated approach, underscoring the need for holistic research to effectively address consumer concerns regarding privacy and security. Previous research has applied traditional AHP methods to contexts such as social media privacy (Liu et al., 2022; Falana et al., 2024), mobile payment systems (Cavus & Adeoluwa, 2022), and cloud computing (Khan et al., 2024). In contrast, this study is the first to examine privacy

and security in platform business models using the FAHP. Unlike conventional AHP-based evaluations, the fuzzy approach incorporates expert confidence levels, enhancing prioritization by accounting for ambiguity and ensuring consistency. By focusing on platform businesses—a domain not previously explored with these methods—this research contributes novel insights to an increasingly dominant model in the digital economy.

Based on the works of Cao et al. (2022), Wisniewski and Page (2022) and Sargiotis (2024), a summary of sub-criteria under the consumer privacy and security evaluation main criteria are shown in
Table *1*. In addition, the last column cites additional literature that helps establish a relationship between the main criteria and sub-criteria.

Table 1
Summary of consumer privacy and security evaluation main criteria and sub-criteria

Main criteria	**Sub-criteria**	**Description of sub-criteria**
Data Collection Practices	Transparency	How clearly the platform communicates its data collection practices to users. Transparency involves clearly communicating how data is collected, used, and shared, ensuring that consumers are fully informed and can give their informed consent. This openness not only fosters trust but also aligns with regulatory requirements and ethical standards (Rahnama & Pentland, 2022).
	Consent	The mechanisms for obtaining user consent for data collection. Consent management involves informing users about data collection practices, allowing them to opt-in or out, and documenting their choices to maintain transparency and accountability. Effective consent practices not only help platforms comply with legal requirements but also build trust with users by respecting their privacy preferences (Palmer, 2021).
	Minimization	Collecting only the data necessary for the platform's operation. By focusing on minimal data collection, platforms can enhance user trust, reduce the risk of data breaches, and comply more easily with stringent data protection regulations (Khan, 2021)
Data Storage and Protection	Purpose Limitation	Ensuring data is used only for the purposes stated at the time of collection. It helps in building a sustainable relationship with users,

Main criteria	Sub-criteria	Description of sub-criteria
		who are increasingly concerned about their privacy and the security of their personal information (Täuscher & Laudien, 2018).
	Data Sharing	Policies regarding sharing data with third parties. Platforms should ensure that data sharing agreements are clear and transparent, outlining the specific purposes for which data will be used. Implementing robust security measures, such as encryption and access controls, is essential to protect data from unauthorized access. Additionally, compliance with data protection regulations (Fassnacht, et al., 2024).
	User Control	Allowing users to control how their data is used and shared. Best practices include providing clear and accessible tools for users to manage their data, such as consent management platforms (CMPs) that allow users to easily grant, withdraw, or modify their consent for data processing (Martín-Peña et al., 2024)
Compliance and Regulatory Framework	Regulatory Compliance	Adherence to relevant laws and regulations (e.g., PDPA). Compliance not only helps avoid hefty fines and legal repercussions but also enhances the platform's reputation by demonstrating a commitment to user privacy and data security (Eke & Stahl, 2024; Taherdoost, 2023).
	Audits and Accountability	Regular audits and accountability measures to ensure compliance and standards maintained in the platform (Padilla et al. 2022). Accountability mechanisms, including transparent reporting and clear data governance policies, further enhance trust by demonstrating a platform's commitment to protecting user information (Eke & Stahl, 2024; Al-Rashdi et al., 2015)
User Awareness and Education	Privacy Policies	Clear and accessible privacy policies. These serve as a transparent declaration of how user data is collected, used, and protected, thereby building trust and ensuring compliance with regulations (McKinsey & Company, 2022).
	User Education	Initiatives to educate users about privacy and security practices. This awareness helps mitigate risks associated with data breaches and misuse, as users can better manage their privacy

Main criteria	Sub-criteria	Description of sub-criteria
		settings and recognize potential threats[1]. Additionally, platforms that invest in user education foster a culture of trust and transparency, which can enhance user loyalty and compliance with privacy regulations (Stabauer, 2019).
Incident Response Management	Breach Notification	Procedures for notifying users in the event of a data breach. Timely and transparent breach notifications allow affected individuals to take necessary actions to protect themselves, such as changing passwords or monitoring their accounts for suspicious activity (Sargiotis, 2024).
	Incident Response Plan	A plan for responding to security incidents. It ensures that all stakeholders are aware of their roles and responsibilities, which enhances coordination and efficiency during a crisis.
Trust & Reputation	User Trust	Building and maintaining user trust through transparent and ethical practices. Trust influences user engagement and loyalty, as consumers are more likely to interact with platforms they perceive as secure and respectful of their privacy (Cao. et al., 2022)
	Reputation Management	Strategies for managing the platform's reputation regarding privacy and security. Effective reputation management involves transparent communication about data practices, swift responses to data breaches, and adherence to privacy regulations (Soleimani, 2022).

The literature on scoring-based decision models for the purpose of evaluating consumer security and privacy of this increasingly important business is still emerging. Even though Table 1 lists both main criteria and sub-criteria for evaluation of consumer security and privacy of platform business models, this study focuses only on main criteria. Our research is based in the Sri Lankan context, and Sri Lanka does not have a mature market for platform businesses. Hence, it is justifiable that determination of weights for main criteria (in the Sri Lankan Context) substantially contributes to the existing body of knowledge.

2.3 Evaluation criteria for consumer privacy and security

The difficulty of criteria selection processes has led to widespread research in decision framework development across various domains. Peppard and Ward (2016) suggest that effective selection frameworks must consider multiple factors including technical capabilities, organizational fit, and long-term sustainability. In particular, this is crucial in

an enterprise setting where multiple stakeholders and requirements must be considered concurrently. The literature reveals the effectiveness of MCDM methods such as the AHP, TOPSIS and ELECTRA, in addressing such complex selection processes. In particular, these methods provide systematic approaches to evaluating alternatives against multiple, often conflicting, criteria while considering diverse stakeholder perspectives (Kumar et al., 2017; Aruldoss et al., 2013). Within the realm of MCDM methods, fuzzy logic approaches have become popular in criteria selection processes. This is due to their ability to handle uncertainty and subjective judgments. Tsai et al. (2010) show the effectiveness of the Fuzzy Delphi method in consolidating expert opinions and achieving consensus on selection criteria. Analogously, Kahraman et al. (2004) have shown how the FAHP can be used to prioritize selection criteria while accounting for the inherent ambiguity in decision-making processes. Van Laarhoven and Pedrycz (1983) used Fuzzy Delphi to systematically collect and consolidate expert opinions, and then applied the FAHP to evaluate and prioritize selection criteria.

Despite advancements in methodology and the growing emphasis on consumer privacy and security within platform business models, a significant gap persists in the development of structured frameworks for evaluating these criteria. Existing literature offers foundational perspectives on privacy concerns through established models. For instance, Westin (2000) introduced a typology categorizing individuals as privacy fundamentalists, pragmatists, or the unconcerned, based on their attitudes toward data sharing. Building on this, Solove (2006) proposed a taxonomy of privacy harms encompassing the following four domains: information collection, processing, dissemination, and invasion. In parallel, security risks are commonly assessed using the CIA triad—confidentiality, integrity, and availability—which serves as a cornerstone for evaluating data protection measures (Whitman & Mattord, 2022). Collectively, these frameworks provide valuable insights into privacy and security issues in digital environments. However, prior studies addressing consumer privacy and security in platform business models (Gurung & Raja, 2016) often focus on isolated elements rather than offering a comprehensive evaluation framework.

The framework proposed in this study seeks to bridge this gap by integrating privacy and security dimensions specific to platform business models, including user education, regulatory compliance, and trust management—factors not explicitly addressed in Westin's or Solove's models. This need becomes increasingly critical given the complexity of consumer risk behaviors and the pivotal role of privacy and security in sustaining platform ecosystems (Chang et al., 2005). To address this challenge, the study applies the FAHP to evaluate consumer privacy and security criteria within platform business models. While the traditional AHP has been employed in contexts such as social media privacy, mobile payment systems, and cloud computing, its fuzzy extension remains unexplored in this domain. The FAHP offers a novel approach by incorporating expert confidence levels, thereby improving prioritization and accounting for ambiguity. This contribution not only advances theoretical understanding but also delivers practical guidance for organizations seeking systematic evaluation methodologies.

3. Methodology

Ranking the criteria of consumer privacy and security aspects of the platform business model identified in the literature survey involves evaluating a set of criteria and prioritizing them based on the stakeholder preference. This can be a complex and multi-dimensional problem. MCDM is a widely used framework for evaluating and selecting criteria. Bhola et al. (2023) argue that MCDM can capture the diverse perspectives and preferences of stakeholders. Thus, MCDM can be thought of as a tool that enables a participatory and inclusive decision-making process.

MCDM is a sophisticated decision-making tool that incorporates both quantitative and qualitative elements (Aruldoss at al 2013; Kumar et al, 2017; Taherdoost, 2023). It is an area of operations research that focuses on developing computational and mathematical tools to assist decision-makers in subjectively evaluating performance criteria.

The optimization literature predominantly references several MCDM methods, including the AHP (Saaty, 1977), Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) (Behzadian et al., 2012), Fuzzy AHP, Elimination and Choice Expressing Reality (ELECTRE) (Roy, 1991), and grey theory (Aruldoss et al., 2013). According to Majumder (2015), MCDM approaches can be broadly categorized into compensatory methods, such as the AHP, and outranking methods, exemplified by ELECTRE, for determining the weights of alternatives. Ciurea and Filip (2015) have applied MCDM techniques to the evaluation of ICT platforms for creative digital works, while Van Looy et al. (2017) developed a MCDM-based decision tool for selecting business process maturity models.

Kabir and Hasin (2011) highlight a limitation of the conventional AHP, noting its reliance on an unbalanced scale of judgment and its inability to adequately address the uncertainty inherent in translating expert judgments into numerical values. Consequently, the AHP may fall short of fully capturing the preferences of decision makers. To address this limitation, fuzzy set theory can be integrated into the pairwise comparison process, thereby accommodating the uncertainty present in human preferences (Liu et al., 2020).

This study deploys the FAHP, a widely used multi-criteria decision-making model, to evaluate platform business models. An overview of the solution approach is shown in Figure 1.

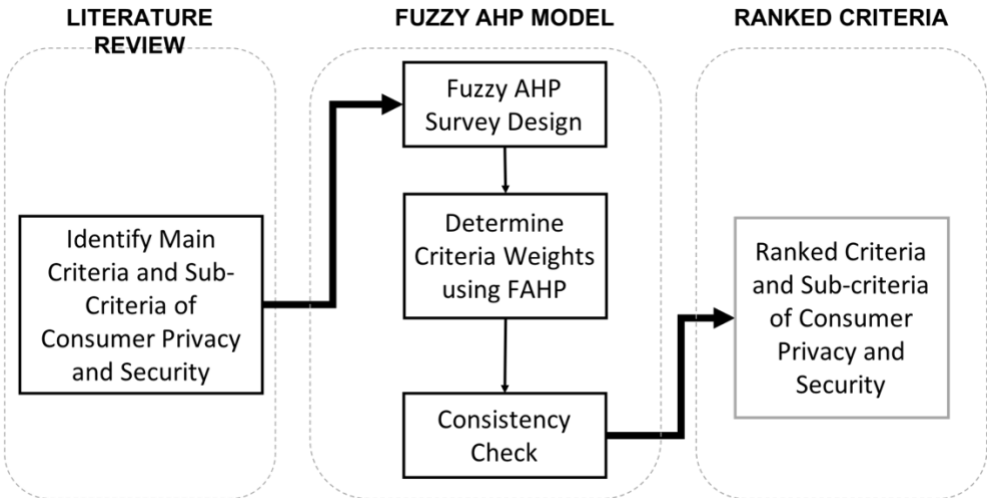

Figure 1 Overview of solution approach

4. Analytical Hierarchy Process (AHP) and Fuzzy Analytical Hierarchy Process (FAHP)

Saaty (1977) introduced the AHP, a structured methodology designed to facilitate complex decision-making. The AHP operates by conducting pairwise comparisons among criteria, sub-criteria, and alternatives, enabling the derivation of relative weights that reflect the importance of each element within the decision hierarchy. Through this process, the AHP generates a prioritized ranking of alternatives based on the aggregated weights assigned to each criterion.

A key feature of the AHP is its ability to capture the relative importance between elements through systematic pairwise comparisons, thereby providing a transparent and rational basis for decision-making. Rather than prescribing a singular "correct" decision, the AHP supports decision-makers in identifying the alternative that most closely aligns with their objectives and preferences.

The hierarchical structure of the AHP allows it to effectively address multi-attribute, multi-stakeholder, and multi-period decision problems. This versatility has led to its widespread application across diverse domains, including business planning, resource allocation, priority setting, and the selection of alternatives. Vaidya and Kumar (2006) conducted a comprehensive review of AHP applications, highlighting its adaptability and utility in various disciplinary contexts.

In this article, we propose a fuzzy theory based AHP to evaluate the influence of the firm's criteria on privacy and security. The FAHP involves the following steps: define the goal, structure the hierarchy from the top level (e.g., goal) through the intermediate levels (criteria and sub-criteria) to the lowest level (alternatives), perform fuzzy pairwise

comparisons to establish priorities among the elements, and synthesis fuzzy judgments to determine an overall ranking (Wind & Saaty, 1980; Van Laarhoven & Pedrycz, 1983). The steps in the FAHP analysis are given as follows:

Step 1
Identify the criteria and sub-criteria used to evaluate the alternatives. These criteria are then structured in a hierarchical format (see Figure 2), which allows for a systematic evaluation of the problem by considering both qualitative and quantitative aspects of the decision (Saaty, 2008; Ishizaka & Labib, 2011).

The basic components/building blocks for the privacy and security enablement in platform business models, are derived from the literature. The essential consumer privacy and security criteria and sub-criteria that can be employed to assess the consumer trust, compliances and ethical considerations of a platform business model are outlined in Table 2.

Table 2
Consumer privacy and security criteria and sub-criteria

Main Criteria, C_i	**Sub-criteria C_{ij}**
Data Collection Practices: $(C_1) \rightarrow \omega_1$	Transparency $(C_{11}) \rightarrow \omega_{11}$
	Consent $(C_{12}) \rightarrow \omega_{12}$
	Minimization (C13) $\rightarrow \omega_{13}$
Data Storage and Protection: $(C_2) \rightarrow \omega_2$	Purpose Limitation $(C_{21}) \rightarrow \omega_{21}$
	Data Sharing $(C_{22}) \rightarrow \omega_{22}$
	User Control $(C_{23}) \rightarrow \omega_{23}$
Compliance and Regulatory Framework: $(C_3) \rightarrow \omega_3$	Regulatory Compliance $(C_{31}) \rightarrow \omega_{31}$
	Audits and Accountability $(C_{32}) \rightarrow \omega_{32}$
User Awareness and Education: $(C_4) \rightarrow \omega_4$	Privacy Policies $(C_{41}) \rightarrow \omega_{41}$
	User Education $(C_{42}) \rightarrow \omega_{42}$
Incident Response Management: $(C_5) \rightarrow \omega_5$	Breach Notification: $(C_{51}) \rightarrow \omega_{51}$
	Incident Response Plan: $(C_{52}) \rightarrow \omega_{52}$

Trust & Reputation: $(C_6) \rightarrow \omega_6$	User Trust: $(C_{61}) \rightarrow \omega_{61}$
	Reputation Management $(C_{62}) \rightarrow \omega_{62}$

Figure 2 shows the 3-level hierarchical structure of main criteria, sub-criteria and alternatives. ω_i and ω_{ij} denote relative importance weights among the main criteria (C_i) and sub-criteria (C_{ij}). i and j represent the number of main and sub-criteria. Weight is computed using the pair-wise comparison responses given by the industry experts.

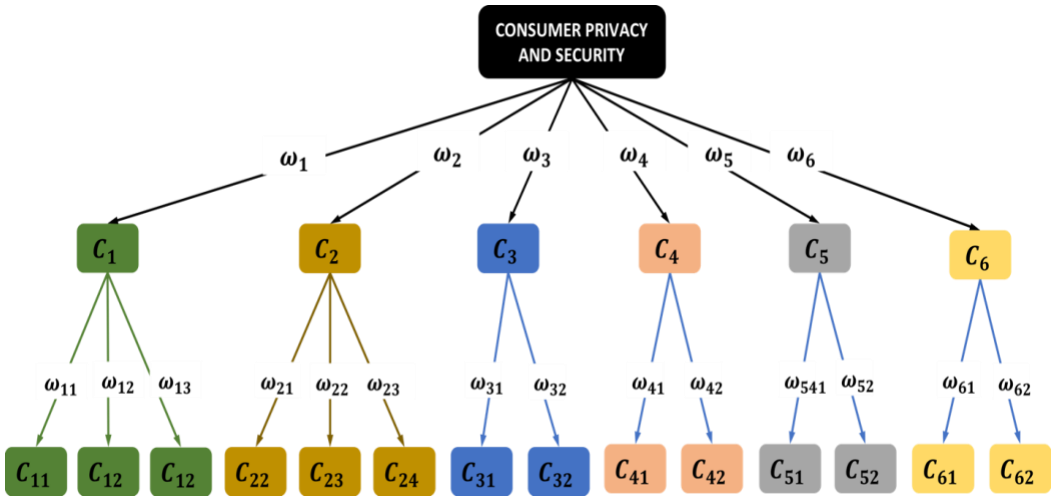

Figure 2 AHP hierarchical structure for consumer trust and security

By incorporating fuzzy logic, the pairwise comparisons in the FAHP capture the ambiguity and uncertainty in expert judgments more effectively, providing a more accurate and reliable assessment of the criteria's relative importance.

Step 2

Complete a pariwise comparison of the criteria. For example, $C_i \succ C_j$ denotes the decision maker's preference for criteria, C_i over the criteria, C_j. Her pairwise comparison value between criteria i and criteria j is c_{ij}. A pairwise comparison matrix can be constructed to record all responses of the decision maker as shown in Equation (1).

$$C = \left[1\ c_{12}\ \ c_{1n}\ c_{21}\ 1\ c_{ij}\ ..\ \ c_{ji} = \frac{1}{c_{ij}}\ 1\ ..\ c_{n1}\ \ 1\right]_{n,n} \quad (1)$$

Following Saaty's work, this study adopts a linear 1 to 9 judgment scale to record the pairwise responses of decision makers (see Table 3)

Table 3
Linear scale used in the AHP

Intensity of importance	Definition	Explanation
1	Equal importance	Two criteria are equally important
3	Moderate importance	One of the criteria is slightly more important than the other
5	Strong importance	One of the criteria is strongly more vital than the other
7	Very Strong importance	One of the criteria is very strongly favored over the other and its dominance is demonstrated in practice
9	Extreme importance	The evident importance of one of criterion over another is of the highest possible order of affirmation which cannot be comparable

Therefore, a pairwise comparison value, c_{ij} can be expressed as: $c_{ij} = \alpha.x \; \forall \; \alpha > 0; x = \{1,2,3,4, \dots ,9\}$.

Gathering expert opinions on the relative importance of each criterion and sub-criterion involved the creation of a survey utilizing the pairwise comparison method. The experts provided their responses on the relative importance of each main criteria against the others based on a linear Likert scale with values ranging from 1 to 9 as proposed by Wind & Saaty (1980) (see Table 4).

Table 4
Sample pairwise comparison survey

Criteria 1	Pairwise comparison - Relative importance																	Criteria 2
Data Collection Practices	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Data Storage and Protection

These responses can be interpreted as such; choosing a rating of 7 in the direction of Criteria 2 means that Criteria 2 is the most important of the two criteria and the level of relative importance is high.

Step 3
Fuzzify the pairwise comparison matrix. Convert the linguistic term into a membership function. Here, we use a triangular membership function. For example, $\mu(A)$ represents the fuzzy value of fuzzy numbers $l, m,$ and n: $\mu(A) = \tilde{A} = (l, m, n)$. l, m and n represent lower, middle and upper ends of the triangular membership function.

Table 5
Fuzzy scale of relative importance

Intensity of importance	Fuzzy number	Fuzzy Value	Definition	Explanation
1	(1,1,1)	$\mu(1)$	Equal importance	Two criteria are equally important
2	(1,2,3)	$\mu(2)$		
3	(2,3,4)	$\mu(3)$	Moderate importance	One of the criteria is slightly more important than the other
4	(3,4,5)	$\mu(4)$		
5	(4,5,6)	$\mu(5)$	Strong importance	One of the criteria is strongly more vital than the other
6	(5,6,7)	$\mu(6)$		
7	(6,7,8)	$\mu(7)$	Very strong importance	One of the criteria is very strongly favored over the other and its dominance is demonstrated in practice
8	(7,8,9)	$\mu(8)$		
9	(8,9,9)	$\mu(9)$	Extreme importance	The evident importance of one criterion over another is of the highest possible order of affirmation which cannot be comparable

Table 5 shows the fuzzified pairwise matrix by replacing each pairwise value with a fuzzy number: $c_{ij} \leftarrow A_{ij} = (l, m, u)$ or $\frac{1}{c_{ij}} \leftarrow A_{ij}^{-1} = \left(\frac{1}{u}, \frac{1}{m}, \frac{1}{l}\right)$. Following Buckley (1985), the row vector geometric mean can be expressed as:

$$\tilde{Z}_i = (A_{i1} \otimes A_{i2} \otimes A_{i3} \otimes A_{i4} \dots \otimes A_{in})^{1/n} \; \forall i. \tag{2}$$

Step 4
Calculate fuzzy weights in the following ways:

$$\tilde{\omega}_i = \tilde{Z}_i \otimes \left(\tilde{Z}_{1j} \oplus \tilde{Z}_{2j} \oplus \tilde{Z}_{3j} \oplus \dots \dots \oplus \tilde{Z}_{nj}\right)^{-1} \forall j. \tag{3}$$

Step 5
Mean of row, i (fuzzy weights) computes the weight of criteria c_i (Centre of Area):

$$\underline{\omega_i} = \frac{\sum_i^n \widetilde{\omega}_i}{n} \quad (4)$$

Step 6

Calculate a Consistency Ration (CR). Saaty (2008) emphasizes the importance of considering the accuracy and reliance of the result derived from the AHP tool and proposes the use of a consistency calculation to overcome the above doubt. The purpose of the consistency calculation is to identify the accuracy of the obtained results. It mainly focuses on identifying the variation of the definition with respect to the practical situations. Equations (5) and (6) were used to determine the CR to identify the consistency of weights. According to Saaty (2008), if the CR is less than or equal to 0.100, then the data are considered consistent.

$$Consistency\ Ratio\ (CR) = \frac{Consistency\ Index\ (CI)}{Random\ Index\ (RI)} \quad (5)$$

$$CI = \frac{(\lambda_{max} - n)}{(n-1)},\ \lambda_{max} = Maximal\ Eigen\ Value\ of\ A \quad (6)$$

The Random Index (RI) is an experimental value that depends on *n*. Saaty and Vargas, (1991) explained the following RI Index for the AHP analysis (see Table 6).

Table 6
RI values for *n* items being compared

N	1	2	3	4	5	6
RI	0	0	0.58	0.90	1.12	1.24

Source: Saaty et al. (2012)

5. Results

5.1 Sampling framework

The literature provides extensive discussion on sample size considerations in the AHP. Unlike other MCDM and statistical methods, the AHP does not require a statistically significant sample size (Dias & Ioannou, 1996). This is because the AHP relies on expert judgments, and a single qualified expert can offer highly representative insights (Tavares et al., 2008). Conversely, larger samples may introduce inconsistencies due to the inclusion of non-experts (Cheng et al., 2002). Consequently, the AHP has gained popularity for developing decision-support models, particularly in contexts where small, specialized panels are appropriate.

The quality of AHP outputs, however, depends on the expertise and diversity of the respondents. To ensure rigor, this study selected 12 industry professionals from eight companies, all possessing substantial experience and recognized certifications in digital

platform security. Thirty percent of the experts were female, and all had a minimum of five years of practical involvement in IT security across Sri Lankan and international firms (Okoli & Pawlowski, 2004; Rowe & Wright, 1999). In addition to bachelor's degrees, most participants held advanced professional credentials such as CISA, CISM, CISSP, and ISO 27001. Responses from two experts were excluded due to evident inconsistencies, resulting in a final panel of 10 experts.

The use of small expert panels in AHP studies is well-supported in prior research, particularly when participants possess deep domain expertise. For example, D'Adamo et al. (2023) successfully applied the AHP with 10 academic experts to prioritize sustainability criteria, while Camcı et al. (2021) achieved robust results using only five construction professionals. Similarly, studies by Prayogo et al. (2024) and Khan et al. (2024) justify small samples by emphasizing methodological precedent and the importance of judgment consistency. These examples affirm that panels of 10 or fewer highly qualified experts can yield valid and reliable AHP outcomes, especially in exploratory or specialized decision-making contexts. In Sri Lanka, the pool of qualified professionals in privacy and security remains limited, as the country is still developing its regulatory frameworks. However, expertise in this domain is gradually expanding as platform-based businesses increasingly recognize the need for specialists in data protection and cybersecurity.

A pairwise comparison of the main criteria based on responses from the 10 selected experts is presented in Table 7.

Table 7
Pairwise comparison of main criteria

	Data Collection Practices	Data Storage and Protection	Compliance & Regulatory Framework	User Awareness and Education	Incident Response Management	Trust & Reputation
Data Collection Practices	1	1/5	1/5	1/5.8	1/5	1/3.75
Data Storage and Protection	5	1	1/3.75	1/5.8	1/5.8	4
Compliance and Regulatory Framework	5	3.75	1	5	3	4
User Awareness and Education	5.8	5.8	1/5	1	4	5
Incident Response Management	5	5.8	1/3	¼	1	1/1.5
Trust & Reputation	3.75	¼	¼	1/5	1.5	1

ISSN 1936-6744
https://doi.org/10.13033/ijahp.v18i1.1346

Since response values are highly fluctuating, the geometric mean value of the pairwise response data sheet has been placed in the upper triangle cells in Table 8 and the lower triangle cells consist of the reciprocal values of each pair. Table 8 computes the fuzzy geometric means of the pair-wise responses of experts based on the Equation (2).

Table 8
Fuzzified pairwise comparison matrix

	Data Collection Practices	Data Storage and Protection	Compliance and Regulatory Framework	User Awareness and Education	Incident Response Management	Trust & Reputation	Fuzzy Geometric Mean $\tilde{Z}_i$
Data Collection Practices	(1,1,1)	(1/6,1/5,1/4)	(1/6,1/5,1/4)	(1/7,1/6,1/5)	(1/6,1/5,1/4)	(1/5,1/4,1/3)	(0.23,0.26,0.33)
Data Storage and Protection	(4,5,6)	(1,1,1)	(1/5,1/4,1/3)	(1/7,1/6,1/5)	(1/7,1/6,1/5)	(3,4,5)	(0.60,0.72,1.47)
Compliance and Regulatory Framework	(4,5,6)	(3,4,5)	(1,1,1)	(1/3,1/2,1/1)	(1,2,3)	(3,4,5)	(1.51,2.08,3.62)
User Awareness and Education	(5,6,7)	(5,6,7)	(1/6,1/5,1/4)	(1,1,1)	(2,3,4)	(4,5,6)	(1.79,2.18,3.48)
Incident Response Management	(4,5,6)	(5,6,7)	(1/2,1/3,1/4)	(1/3,1/4,1/5)	(1,1,1)	(1/3,1/2,1/1)	(1.02,1.04,1.48)
Trust & Reputation	(3,4,5)	(1/5,1/4,1/3)	(1/5,1/4,1/3)	(1/6,1/5,1/4)	(1,2,3)	(1,1,1)	(0.52,0.68,1.09)

Table 9 below shows crisp/defuzzied weights derived from fuzzy weights following Equation (3).

Table 9
Fuzzy weights and weights

Criteria	**Fuzzy Weights, $\widetilde{\omega}_i$**	**Centre of Area (Weight, ω_i)**	**Conventional AHP weights**
Data Collection Practices (ω_1)	(0.23,0.26.0.33)⊗(1/5.68,1/6.96,1/11,47) = (0.04, 0.04, 0.03)	3.56%	6.30%
Data Storage and Protection (ω_2)	(0.60,0.72,1.47)⊗(1/5.68,1/6.96,1/11.47) = (0.11,0.10,0.13)	11.27%	10.48%
Compliance and Regulatory Framework (ω_3)	(1.51,2.08,3.62)⊗(1/5.68,1/6.96,1/11.47) = (0.27,0.30,0.32)	29.35%	41.55%
User Awareness and Education (ω_4)	(1.79,2.18,3.48)⊗(1/5.68,1/6.96,1/11.47) = (0.32,0.31,0.30)	29.09%	22.49%
Incident Response Management (ω_5)	(1.02,1.04,1.48)⊗(1/5.68,1/6.96,1/11.47) = (0.18,0.15,0.13)	15.25%	15.89%
Trust & Reputation (ω_6)	(0.52,0.68,1.09)⊗(1/6.68,1/6.96,1/11.47) = (0.09,0.10,0.09)	9.49%	3.29%

Normalized weights of the FAHP and weights of the conventional AHP are shown in the right-hand columns of Table 9. However, significant judgment errors in AHP pairwise comparisons mainly stem from cognative limitations of the experts.

The FAHP provides an average λ value of 7.017 resulting in a CR of 0.16 (~ 0.100). Therefore, the results of the analysis could be considered consistent. Since the weights derived for each main criterion fulfill the requirement of a consistent ratio, the following results explain the criteria to be considered when making decisions related to privacy and security aspects of digital business platforms.

The aggregated pairwise comparison matrix yielded a eigenvalue λ_max = 8.06, from which the CI of 0.203 was computed. With a RI of 1.24 for a 6 x 6 matrix, the CR = 0.16 (which marginally meets the 0.1 threshold, indicating acceptable consistency).

The FAHP analysis indicates two dominant criteria. User Awareness and Education (~31%) and Compliance and Regulatory Framework (~30%) capture the majority of the importance weight, together accounting for ~61% of the total. The remaining four criteria

share roughly 39%, with Data Collection Practices notably the lowest (around 3–4%).

6. Discussion

6.1 User awareness and education

Consumer awareness and education are essential elements in platform business models to ensure privacy and security. Effective educational campaigns can enable individuals to make educated decisions on their data. Prince et al. (2024) assert that augmenting online privacy literacy via declarative and procedural knowledge substantially enhances users' information privacy empowerment. Rahnama and Pentland (2022) assert that platforms must foster trust through transparent communication of data use policies and prioritize the extraction of insights over personally identifiable information. These measures are crucial for cultivating a secure and reliable digital environment. Out of all six criteria considered, Consumer Awareness and Education is considered the most important criteria, which constitutes 31.09% significance to the overall consumer privacy and security of the platform business models.

User awareness and education showed a difference between the AHP and FAHP outputs likely because experts expressed varying degrees of confidence in its importance. The FAHP captured this uncertainty through fuzzy scales, resulting in a more moderated weight compared to the AHP's crisp prioritization, which may result in an amplified consensus without accounting for hesitation.

6.2 Compliance and regulatory framework

Compliance and regulatory frameworks are crucial in platform business models to ensure consumer privacy and security. These frameworks often include adherence to laws such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), which mandate stringent data protection measures. According to Mattsson (2020), compliance with these regulations involves implementing advanced data security solutions and de-identification techniques to protect sensitive information. Furthermore, Rahnama and Pentland (2022) highlight the importance of cultivating trust with consumers by being transparent about data usage and focusing on extracting insights rather than personal identifiable information. Sri Lanka's Personal Data Protection Act (PDPA), enacted in March 2022, represents a significant step towards comprehensive data privacy legislation in South Asia. This Act imposes stringent requirements on platform business models, necessitating robust data protection measures to ensure compliance. According to Greenleaf (2022), the PDPA includes provisions for a new Data Protection Authority with broad enforcement powers, similar to the GDPR. Fernando and Wickramasinghe (2022) highlight that the Act's extra-territorial scope and data localization requirements will particularly impact platforms operating across borders, compelling them to adopt enhanced data security practices. These regulatory changes are crucial for protecting consumer privacy and fostering trust in digital platforms. Considering its financial impact due to data breaches and potential litigations, the study outcomes show Data protection and regulatory framework to be a key dimension owning to a weightage of 29.35% in ensuring consumer

privacy and security in platform business models. Compliance and regulatory framework may have received a higher FAHP weight due to statistical analysis process inherent to the FAHP when accommodating nuanced expert views—especially in an emerging regulatory environment such as Sri Lanka—where experts might agree on its importance but differ on how strongly they perceive its immediate impact.

6.3 Incident response management

Incident response management was deemed to be moderately important with a relative importance of 15.25% compared to other criteria to ensure consumer privacy and security in platform business model.

Incident response management likely saw output differences because experts may have had mixed opinions on its operational readiness across platforms. The FAHP allowed these subtleties to be reflected in the final weights, whereas the AHP treated all judgments as equally confident, potentially skewing the result toward a more definitive ranking.

6.4 Data storage and protection

Data storage and protection are critical components of modern data management practices, ensuring the integrity, confidentiality, and availability of data. Effective data storage involves using reliable and scalable solutions such as cloud storage, which offers flexibility and cost-efficiency. However, it also necessitates robust security measures be implemented in order to protect sensitive information from unauthorized access and breaches. According to Altman et al. (2018), the increasing complexity of data storage systems, driven by advancements in technology, requires sophisticated privacy controls to mitigate long-term risks. Tenopir et al. (2020) highlight that while many researchers are willing to share their data, there is a significant need for better long-term storage solutions and data management practices to facilitate data reuse and ensure security. These insights underscore the importance of adopting comprehensive data protection strategies to safeguard information in an increasingly data-driven world. Data storage and protection measures are deemed to be moderately important and have a relative importance of 11.27% compared to other criteria to ensure consumer privacy and security in platform business models.

6.5 Trust and reputation

Trust and reputation are critical in platform business models to ensure consumer privacy and security. Effective trust-building strategies include transparent communication about data practices and robust security measures. According to Fox et al. (2022), the implementation of GDPR privacy labels significantly enhances consumer perceptions of privacy and trust, leading to increased willingness to share data. Soleimani (2022) emphasizes that trust in e-commerce platforms reduces perceived risks and is essential for successful online transactions. These insights highlight the importance of fostering trust through clear privacy policies and strong data protection practices to maintain consumer confidence in digital platforms. Based on AHP analysis done to evaluate the firm criteria influence on privacy and security, data collection practices scores a 9.49% relative

importance compared to other criteria that contribute to consumer privacy and security. This dimension exhibits a low importance in terms of the fuzzy weights analyzed.

6.6 Data collection practices

In platform business models, data collection strategies must reconcile the necessity for useful customer insights with rigorous privacy and security protocols. Effective measures encompass limiting data gathering to essential information, utilizing strong encryption techniques, and maintaining transparency regarding data utilization. Padilla et al. (2022) assert that platforms employing a hybrid model, which integrate intermediation with proprietary offerings, frequently have heightened difficulties in preserving consumer privacy due to augmented data collecting requirements. Quach et al. (2022) underscore the significance of regulatory compliance, including adherence to GDPR and other privacy legislation, to safeguard consumer data and foster confidence. These procedures are essential for alleviating privacy issues and improving the security of customer data in the platform business architectures. Based on the AHP analysis done to evaluate the firm criteria influence on privacy and security, Data collection practices scores a 3.84% relative importance compared to other criteria that contribute to consumer privacy and security. This dimension exhibits the lowest importance in terms of the fuzzy weights analyzed.

7. Conclusions

7.1 Summary and key findings

The application of the FAHP in this study revealed that two criteria—user education and regulatory compliance—are particularly critical for strengthening privacy and security in platform business models. These findings underscore the strategic need for platforms to prioritize these areas to enhance user trust. Importantly, the FAHP enabled the incorporation of expert uncertainty into the decision-making process, ensuring consistency across judgments ($CR \approx 0.1$) and lending robustness to the results.

7.2 Theoretical and practical contributions

This research emphasizes the necessity for platforms to balance data utilization with ethical and regulatory obligations, proposing a framework that integrates privacy-preserving technologies and principles of ethical data governance. However, several limitations must be acknowledged. First, the study lacks empirical validation (Acquisti et al., 2015) and is constrained by a narrow industry scope (Martin & Murphy, 2017). Second, assumptions regarding technological and operational feasibility—such as cost, scalability, and user adoption—were not fully examined (Zhou et al., 2020). Third, the analysis reflects current regulatory regimes (e.g., GDPR, CCPA, PDPA–Sri Lanka) without accounting for the evolving nature of global privacy laws, which may affect the long-term applicability of recommendations (Taddeo & Floridi, 2018).

7.3 Methodological considerations and limitations of FAHP

While the FAHP offers a robust mechanism for managing uncertainty in expert-driven evaluations, it is not without limitations. The assignment of fuzzy numbers is inherently

subjective, and the absence of a universally accepted ranking method can introduce inconsistencies. Furthermore, the FAHP does not allow criteria to receive a zero weight, even when their relevance is minimal. Assessing consistency in fuzzy pairwise comparisons is also more complex than in the traditional AHP. Ultimately, the reliability of the FAHP outcomes depends heavily on expert competence and familiarity with both the domain and the FAHP methodology.

7.4 Managerial implications

From a strategic perspective, privacy should be viewed as a driver of brand loyalty and competitive advantage (Culnan & Bies, 2003). Managers are encouraged to embed privacy into core business strategies (Shokri & Shmatikov, 2015), invest in privacy-enhancing technologies, and foster cross-functional collaboration for comprehensive data governance (Smith et al., 2011). Ethical leadership and transparent data practices are essential for sustaining user engagement and mitigating reputational risks (Martin, 2018).

7.5 Future research directions

Although 14 sub-criteria were identified during framework development, this study focused exclusively on ranking six main criteria due to scope constraints. Future research should extend the FAHP analysis to sub-criteria for deeper insights. Additionally, given the study's contextual focus on Sri Lanka's platform market, findings are most applicable to similar emerging economies with nascent data protection regimes and limited cybersecurity expertise. Broader generalization requires cross-country studies incorporating diverse regulatory environments and expert pools. Future work could also integrate complementary decision-making techniques such as TOPSIS or DEMATEL to validate and enrich the findings.

The growing integration of Artificial Intelligence (AI) and Generative AI (GenAI) into platform ecosystems introduces both opportunities and challenges for consumer trust and privacy. While AI enables advanced personalization through large-scale data processing, it also raises concerns about security, misuse, and opacity. Chakravorti (2024) highlights trust deficits stemming from disinformation risks, ethical dilemmas, and the "black box" nature of AI. Similarly, Deloitte Insights (2024) stresses the need for trust standards in GenAI to maintain consumer confidence. Future research should explore how transparent and explainable AI practices, coupled with strong regulatory compliance and user education, can mitigate these risks and foster a trustworthy digital environment. Such investigations would provide actionable insights for platform businesses seeking to balance innovation with privacy and security imperatives.

REFERENCES

Abeysekara, T. B., & Ranasinghe, A. E. (2022). Holistic approach in introducing proper legal framework to regulate data protection and privacy in Sri Lanka. *Journal of Business Research and Insights*, *8*(I), 169–200. https://doi.org/10.31357/vjm.v8iI.5608.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514. https://www.cmu.edu/dietrich/sds/docs/loewenstein/PrivacyHumanBeh.pdf

Al-Rashdi, Zahir, Dick, M., & Storey, I. (2015). "A conceptual framework for accountability in cloud computing service provision". *Austrailian Conference on Information Systems 2015 Proceedings*, 76. https://aisel.aisnet.org/acis2015/76

Altman, M., Wood, A., O'Brien, D. R., & Gasser, U. (2018). Practical approaches to big data privacy over time. *International Data Privacy Law, 8*(1), 29–51. https://doi.org/10.1093/idpl/ipx027

Aruldoss, M., Lakshmi, T. M., & Venkatesan, V. P. (2013). A survey on multi criteria decision making methods and its applications. *American Journal of Information Systems, 1*(1), 31–43. https://doi.org/10.12691/ajis-1-1-5

Behzadian, M., Otaghsara, S. K., Yazdani, M., & Ignatius, J. (2012). A state-of the-art survey of TOPSIS applications. *Expert Systems with Applications, 39*(17), 13051–13069. https://doi.org/10.1016/j.eswa.2012.05.056

Bhola, P., Chronis, A. G., Kotsampopoulos, P., & Hatziargyriou, N. (2023). Business model selection for community energy storage: a multi criteria decision making approach. *Energies, 16*(18), 6753. https://doi.org/10.3390/en16186753

Campbell, J. E., & Carlson, M. (2002). Panopticon. com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media, 46*(4), 586–606. https://doi.org/10.1207/s15506878jobem4604_6

Cao, C., Zheng, M., Ni, L. (2022). Improving consumer data privacy protection and trust in the context of the digital platform. In A. Moallem (Ed.) *HCI for cybersecurity, privacy and trust. HCII 2022. Lecture Notes in Computer Science* , *13333*, 16-29. Springer. https://doi.org/10.1007/978-3-031-05563-8_2

Camcı, A., Yıldız, A., & Kılıç, S. (2021). Selection of contract type in construction projects using spherical AHP method. In H. A. Abbass, M. A. Bakar, & M. A. Abdullah (Eds.), *Proceedings of the International Online Conference on Intelligent Decision Science* (pp. 509–518). Springer. https://doi.org/10.1007/978-3-030-66501-2_42

Cavus, N., & Adeoluwa, A. (2022). Security and privacy concerns in mobile payment services. *Global Journal of Information Technology: Emerging Technologies, 12*(2), 82–94. https://doi.org/10.18844/gjit.v12i2.8264

Chakravorti, B. (2024). AI's trust problem. *Harvard Business Review*. https://bpb-us-w2.wpmucdn.com/sites.uab.edu/dist/6/536/files/2024/09/AIs-Trust-Problem.pdf

Chang, M. K., Cheung, W., & Lai, V. S. (2005). Literature derived reference models for the adoption of online shopping. *Information & Management, 42*(4), 543–559. https://doi.org/10.1016/j.im.2004.02.006

Chan, Yolande E. and Greenaway, & Kathleen E. (2005). Theoretical explanations for firms' information privacy behaviors. *Journal of the Association for Information Systems, 6*(6), 171–198. https://doi.org/10.17705/1jais.00068

Cheng, E. W., Li, H., & Ho, D. C. (2002). Analytic hierarchy process (AHP) A defective tool when used improperly. *Measuring Business Excellence, 6*(4), 33–37. https://doi.org/10.1108/13683040210451697

Ciurea, C., & Filip, F. G. (2015). Multi-Criteria Analysis in choosing IT&C platforms for creative digital works. *Uncommon Culture, 6*(2), 20–27. https://journals.uic.edu/ojs/index.php/UC/article/view/6200

Culnan, M. (1993). How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly, 17*(3), 341–362. https://doi.org/10.2307/249775

Culnan, M. J. (2000). Protecting privacy online: Is self-regulation working? *Journal of Public Policy & Marketing, 19*(1), 20–26. https://doi.org/10.1509/jppm.19.1.20.16944

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342. https://doi.org/10.1111/1540-4560.00067

D'Adamo, I., Rosa, P., & Sassanelli, C. (2023). The Analytic Hierarchy Process as an innovative way to enable stakeholder engagement for sustainability reporting in the food industry. *Environment, Development and Sustainability, 25*, 15025–15042. https://doi.org/10.1007/s10668-022-02700-0.

Dias Jr, A., & Ioannou, P. G. (1996). Company and project evaluation model for privately promoted infrastructure projects. *Journal of Construction Engineering and Management, 122*(1), 71–82. https://doi.org/10.1061/(ASCE)0733-9364(1996)122:1(71)

Deloitte Insights. (2024, November 19). *Deepfake disruption: A cybersecurity-scale challenge and its far-reaching consequences*.

https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2025/gen-ai-trust-standards.html

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: A review. *Sensors, 23*(3), 1151. https://doi.org/10.3390/s23031151

DLA Piper. (2023 January). *DLA Piper GDPR fines and data breach survey*. https://www.dlapiper.com/en/insights/publications/2023/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2023

Eke, D., & Stahl, B. (2024). Ethics in the governance of data and digital technology: An analysis of European data regulations and policies. *Digital Society, 3*(1), 11. https://doi.org/10.1007/s44206-024-00101-6.

Falana, O. J., Ojeaga, T., Naeem, H., Aborisade, D. O., Alsirhani, A., Alserhani, F., & Alserhani, F. (2024). FHG-PR: A hybridized fuzzy-AHP and game theory model for assessing privacy risk on social media platforms. *Frontiers in Computer Science, 6*, 1–18. https://doi.org/10.3389/fcomp.2024.1389223

Fassnacht, M., Leimstoll, J., Benz, C., Heinz, D., & Satzger, G. (2024). Data sharing practices: The interplay of data, organizational structures, and network dynamics. *Electronic Markets, 34*(1), 47. https://doi.org/10.1007/s12525-024-00732-0.

Fernando, J., & Wickramasinghe, S. (2022). *Sri Lanka personal data protection legislation–An overview*. https://dx.doi.org/10.2139/ssrn.4246818

Fox, G., Lynn, T. & Rosati, P. (2022). Enhancing consumer perceptions of privacy and trust: a GDPR label perspective. *Information Technology & People, 35*(8), 181–204. https://doi.org/10.1108/ITP-09-2021-0706

Greenleaf, G. (2022). *Sri Lanka's personal data protection act is finalized with a stronger DPA*, 177 Privacy Laws & Business International Report 25-27, UNSW Law Research Paper No. 22–53. http://dx.doi.org/10.2139/ssrn.4181012

Gurung, A. & Raja, M.K. (2016). Online privacy and security concerns of consumers. *Information and Computer Security, 24*(4), 348–371. https://doi.org/10.1108/ICS-05-2015-0020.

Hiller, J. S., & Cohen, R. (2001). *Internet law and policy*. Prentice-Hall.

Ishizaka, A., & Labib, A. (2011). Review of the main developments in the analytic hierarchy process. *Expert Systems with Applications*, *38*(11), 14336-14345. https://doi.org/10.1016/j.eswa.2011.04.143

Kabir, G., & Hasin, M. A. A. A. (2011). Evaluation of customer-oriented success factors in mobile commerce using fuzzy AHP. *Journal of Industrial Engineering and Management (JIEM), 4*(2), 361–386. https://doi.org/10.3926/jiem..v4n2.p361-386

Kahraman, C., Cebeci, U., & Ruan, D. (2004). Multi-attribute comparison of catering service companies using fuzzy AHP: The case of Turkey. *International Journal of Production Economics, 87*(2), 171–184. https://doi.org/10.1016/S0925-5273(03)00099-9

Khan., M. (2021). *Data minimization – a practical approach*. https://www.isaca.org/resources/news-and-trends/industry-news/2021/data-minimization-a-practical-approach

Khan, M. Z., Shoaib, M., Husain, M. S., Ul Nisa, K., & Quasim, M. T. (2024). Enhanced mechanism to prioritize the cloud data privacy factors using AHP and TOPSIS: A hybrid approach. *Journal of Cloud Computing, 13*, 42. https://doi.org/10.1186/s13677-024-00606-y

KPMG. (2024, September), *KPMG global tech report*. https://kpmg.com/kpmg-us/content/dam/kpmg/corporate-communications/pdf/2024/KPMG%20tech%20report%202024_US%20Market.pdf

Kumar, R., Bilga, P. S., & Singh, S. (2017). Multi objective optimization using different methods of assigning weights to energy consumption responses, surface roughness and material removal rate during rough turning operation. *Journal of Cleaner Production, 164*, 45–57. https://doi.org/10.1016/j.jclepro.2017.06.077

Liu, Y., Eckert, C. M., & Earl, C. (2020). A review of fuzzy AHP methods for decision-making with subjective judgements. *Expert Systems with Applications, 161*, 113738. https://doi.org/10.1016/j.eswa.2020.113738

Liu, Y., Tse, W. K., Kwok, P. Y., & Chiu, Y. H. (2022). Impact of social media behavior on privacy information security based on Analytic Hierarchy Process. *Information, 13*(6), 280. https://doi.org/10.3390/info13060280

Lutz, C., Hoffmann, C. P., Bucher, E., & Fieseler, C. (2018). The role of privacy concerns in the sharing economy. Information. *Communication & Society, 21*(10), 1472–1492. https://doi.org/10.1080/1369118X.2017.1339726

Majumder, M. (2015). Multi Criteria Decision Making. In *Impact of Urbanization on Water Shortage in Face of Climatic Aberrations*, SpringerBriefs in Water Science and Technology, (pp. 35–47). Springer. https://doi.org/10.1007/978-981-4560-73-3_2

Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research, 82*, 103–116. https://doi.org/10.1016/j.jbusres.2017.08.034

Martin, K., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 45*(2), 135–155. https://doi.org/10.1007/s11747-016-0495-4

Martín-Peña, M. L., Lorenzo, P. C., & Meyer, N. (2024). Digital platforms and business ecosystems: a multidisciplinary approach for new and sustainable business models. *Review of Managerial Science*, 1-18. https://doi.org/10.1007/s11846-024-00772-y

Mattsson, U. (2020). Practical data security and privacy for GDPR and CCPA. *ISACA Journal, 3*(3). https://www.isaca.org/resources/isaca-journal/issues/2020/volume-3/practical-data-security-and-privacy-for-gdpr-and-ccpa

McKinsey & Company. (2022, April 27). *The consumer data opportunity and the privacy imperative*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*, 119. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

Nooren, P., Van Gorp, N., van Eijk, N., & Fathaigh, R. Ó. (2018). Should we regulate digital platforms? A new framework for evaluating policy options. *Policy & Internet, 10*(3), 264–301. https://doi.org/10.1002/poi3.177

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information & Management, 42*(1), 15–29. https://doi.org/10.1016/j.im.2003.11.002

Palmer, B. W. (2021). Informed consent. In S. Panicker & B. Stanley (Eds.), *Handbook of research ethics in psychological science* (pp. 55–71). American Psychological Association. https://doi.org/10.1037/0000258-004

Padilla, J., Piccolo, S., & Vasconcelos, H. (2022). Business models, consumer data and privacy in platform markets. *Journal of Industrial and Business Economics, 49*(3), 599–634. https://doi.org/10.1007/s40812-022-00218-0.

Peppard, J., & Ward, J. (2016). *The strategic management of information systems: Building a digital strategy*. John Wiley & Sons.

Prince, C., Omrani, N. & Schiavone, F. (2024). Online privacy literacy and users' information privacy empowerment: the case of GDPR in Europe. *Information Technology & People, 37*(8), 1–24. https://doi.org/10.1108/ITP-05-2023-0467

Prayogo, D. H., Santoso, A. S., & Wibowo, A. (2024). The key factors for improving returns management in e-commerce in Indonesia from customers' perspectives—An AHP approach. *Sustainability, 16*(17), 7303. https://doi.org/10.3390/su16177303

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 Scences, 50*, 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Rahnama, H., & Pentland, A. (2022). The new rules of data privacy. *Harvard Business Review*, 25.

Rochet, J. C., & Tirole, J. (2003). Platform competition in two-sided markets. *Journal of the European Economic Association, 1*(4), 990–1029. https://doi.org/10.1162/154247603322493212

Rowe, G., & Wright, G. (1999). The Delphi technique as a forecasting tool: issues and analysis. *International Journal of Forecasting, 15*(4), 353–375. https://doi.org/10.1016/S0169-2070(99)00018-7

Saaty, T. L. (1977). A scaling method for priorities in hierarchical structures. *Journal of Mathematical Psychology, 15*(3), 234–281. https://doi.org/10.1016/0022-2496(77)90033-5

Saaty, T. L., & Vargas, L. G. (1991). *Prediction, projection, and forecasting: applications of the analytic hierarchy process in economics, finance, politics, games, and sports.* SpringerNature Link.

Saaty, T. L. (2008). The analytic hierarchy and analytic network measurement processes: applications to decisions under risk. *European Journal of Pure and Applied Mathematics, 1*(1), 122–196. https://doi.org/10.29020/nybg.ejpam.v1i1.6

Sargiotis, D. (2024). Data security and privacy: Protecting sensitive information. In *Data Governance* (pp. 217–245). Springer. https://doi.org/10.1007/978-3-031-67268-2_6

Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 1310–1321. https://doi.org/10.1145/2810103.2813687

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015. http://dx.doi.org/10.2307/41409970

Soleimani, M. (2022). Buyers' trust and mistrust in e-commerce platforms: a synthesizing literature review. *Information Systems and e-Business Management, 20*(1), 57–78. https://doi.org/10.1007/s10257-021-00545-0

Stabauer, M. (2019). The effects of privacy awareness and content sensitivity on user engagement. In F.H. Nah, K. Siau. (Eds.) *HCI in Business, Government and Organizations. Information Systems and Analytics. HCII 2019. Lecture Notes in Computer Science*, *11589*, 242 – 255. Springer. https://doi.org/10.1007/978-3-030-22338-0_20

Stalla-Bourdillon, S. (2014). *Privacy versus security… are we done yet?*. Springer. https://ssrn.com/abstract=2493109

Solove, D. J. (2006). *A taxonomy of privacy*, 154 U. Pa. L. Rev. 477 (2006). https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1

Su, Y., & Jin, L. (2022). The impact of online platforms' revenue model on consumers' ethical inferences. *Journal of Business Ethics*, 1-15. https://doi.org/10.1007/s10551-021-04798-0

Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science*, *361*(6404), 751–752. https://doi.org/10.1126/science.aat5991

Taherdoost, H. (2023). Legal, regulatory, and ethical considerations in e-business. In *E-Business Essentials. EAI/Springer Innovations in Communication and Computing*, 379–402. Springer. https://doi.org/10.1007/978-3-031-39626-7_15.

Tavares, R. M., Tavares, J. L., & Parry-Jones, S. L. (2008). The use of a mathematical multicriteria decision-making model for selecting the fire origin room. *Building and Environment*, *43*(12), 2090– 2100. https://doi.org/10.1016/j.buildenv.2007.12.010

Täuscher, K., & Laudien, S. M. (2018). Understanding platform business models: A mixed methods study of marketplaces. *European Management Journal, 36*(3), 319–329. https://doi.org/10.1016/j.emj.2017.06.005

Tenopir, C., Rice, N. M., Allard, S., Baird, L., Borycz, J., Christian, L., ... & Sandusky, R. J. (2020). Data sharing, management, use, and reuse: Practices and perceptions of scientists worldwide. *PloS One, 15*(3), e0229003. https://doi.org/10.1371/journal.pone.0229003.

Tsai, H. Y., Chang, C. W., & Lin, H. L. (2010). Fuzzy hierarchy sensitive with Delphi method to evaluate hospital organization performance. *Expert Systems with Applications, 37*(8), 5533–5541. https://doi.org/10.1016/j.eswa.2010.02.099

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*(1), 20–36.

Van Laarhoven, P. J., & Pedrycz, W. (1983). A fuzzy extension of Saaty's priority theory. *Fuzzy Sets and Systems, 11*(1-3), 229–241. https://doi.org/10.1016/S0165-0114(83)80082-7

Van Looy, A., Poels, G., & Snoeck, M. (2017). Evaluating business process maturity models. *Journal of the Association for Information Systems, 18*(6), 1. https://doi.org/10.17705/1jais.00460

Vaidya, O. S., & Kumar, S. (2006). Analytic hierarchy process: An overview of applications. *European Journal of Operational Research, 169*(1), 1–29. https://doi.org/10.1016/j.ejor.2004.04.028

Vijayasarathy, L. R. (2004). Predicting consumer intentions to use on-line shopping: the case for an augmented technology acceptance model. *Information & Management, 41*(6), 747–762. https://doi.org/10.1016/j.im.2003.08.011

Wang, R. J. H. (2020). Branded mobile application adoption and customer engagement behavior. *Computers in Human Behavior, 106*, 106245. https://doi.org/10.1016/j.chb.2020.106245

Westin, A. F. (2000). Intrusions. *Public Perspective, 11*(6), 8–11.

Wind, Y., & Saaty, T. L. (1980). Marketing applications of the analytic hierarchy process. *Management Science, 26*(7), 641–658. https://doi.org/10.1287/mnsc.26.7.641

Wisniewski, P.J., Page, X. (2022). Privacy theories and frameworks. In B.P. Knijnenburg, X. Page, P. Wisniewski, H.R. Lipford, N. Proferes, J. Romano (Eds.) *Modern socio-technical perspectives on privacy* (pp. 15–41). Springer. https://doi.org/10.1007/978-3-030-82786-1_2

Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage.

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

Xu, H., Dinev, T., Smith, H. & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 Proceedings*, 6. https://aisel.aisnet.org/icis2008/6

Zhou, J., Leung, V. C., & Li, H. (2020). Privacy-preserving technologies for smart cities. *IEEE Communications Magazine, 58*(6), 20–26. http://dx.doi.org/10.1109/ACCESS.2018.2853985