MSTS Methods in Science and Technology Studies

futuristech PT. Teknologi Futuristik Indonesia

Received: May 3, 2026; Revised: July 17, 2026; Accepted: July 18, 2026; Published: July 19, 2026; Current version: July 19, 2026. e-ISSN: 3123-4232
Digital Object Identifier 10.64539/msts.v2i2.2026.522

Article

Trust–Privacy-Based User Acceptance Model for Location-Based Mobile Navigation Services: Conceptual Development and Research Propositions

Atta Ur Rahman[1,*], Fuyang Ke[2], Muhammad Raza[3]

[1] School of Computer Science and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China; e-mail: atturrehaman.1990@gmail.com, 202451200014@nuist.edu.cn (A. Ur Rahman).
[2] School of Software, Nanjing University of Information Science and Technology, Nanjing 210044, China; e-mail: kefuyang@nuist.edu.cn (F. Ke).
[3] School of Computer Science, Nanjing University of Information Science and Technology, Nanjing 210044, China; e-mail: 202452200033@nuist.edu.cn (M. Raza).
* Correspondence Author

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Abstract: The two most important factors for location-based mobile navigation services are navigation performance and trusted data governance, especially when location data is used repeatedly. Previous studies have tended to focus on privacy concerns, perceived risk, trust, transparency, control, and service quality separately or in settings other than consumer navigation, as is the case in this study. As a result, the interaction between privacy risk perceptions and provider assurances in influencing mobile navigation acceptance remains poorly defined. This conceptual study develops a trust- and privacy-based user acceptance framework by synthesizing the literature through a structured procedure and incorporating the Technology Acceptance Model, Privacy Calculus Theory, and Trust Theory. The framework posits that privacy concern increases perceived risk, while privacy concern and perceived risk reduce trust. In contrast, transparency, perceived control over location data, and service reliability can enhance trust. The roles of perceived usefulness and user acceptance intention in the pathway to user acceptance remain unchanged, suggesting that trust is an antecedent to perceived usefulness and user acceptance intention. The framework fills the theoretical gap between privacy-risk assessment and trust-building service attributes, and between trust in technology acceptance and repeated disclosure of the location setting. It also recognizes the need for transparent data practices, meaningful location control, and reliable service performance as provisional design priorities, which require future empirical validation. The propositions are to be used as a starting point for further testing on platforms, providers, user groups, cultures, and regulatory frameworks.

Keywords: Location-based mobile navigation services; User acceptance; Privacy concern; Perceived risk; Trust; Data governance.

1. Introduction

Location-based mobile navigation services assist in planning routes, provide real-time guidance, locate sites, estimate travel times, and are widely used for mobility. Their value depends on users' precise or approximate real-time or historical location information, such as background location data or location and movement history. Such data can be utilized to provide information about routes, routines, typical locations, home and work locations, and general behavior [1]–[5]. However, mobile navigation services will only be accepted if they are functional and easy to use, and if users trust how service providers gather, store, share, and secure their location information.

The Technology Acceptance Model (TAM) focuses primarily on perceived usefulness and perceived ease of use in technology adoption [6]. The Unified Theory of Acceptance and Use of Technology (UTAUT) and

UTAUT2 further expand this view with respect to the performance, effort, social, facilitating, motivational, and behavioral factors [7], [8]. They are useful for laying a solid foundation for understanding adoption. However, the original models do not address the vulnerability that arises when sensitive location information must be provided multiple times to deliver a service. The Privacy Calculus Theory can be applied to determine whether or not disclosure is beneficial, with respect to the potential disclosure costs for the individuals [9], [10], and the Trust Theory can be applied to explain the willingness of the users to trust the providers, given their uncertainty and vulnerability [11], [12].

The relevance of beliefs regarding privacy concerns, perceived risk, trust, service quality, and technology acceptance has received empirical support in the context of location-based and mobility-related services in previous studies [13]–[21]. Evidence spans the general use of location-based services, emergencies, and social networking, MaaS, and navigation systems. Consumer mobile navigation is a special instance of double dependency, as it requires a mobile navigation provider to deliver timely and accurate navigation and for the user to take responsibility for handling mobility information. Until now, prior models have not fully explained the mixed situation (negative privacy assessments and positive provider assurances).

The unresolved issue is how privacy-risk factors, trust-building attributes, and technology-acceptance beliefs can be organized into a coherent framework. Instead, it is about putting in place the factors that raise privacy concerns – in a coherent explanatory structure with the build-up factors: trust and technology-acceptance beliefs – in the case of mobile navigation. Evaluations that heighten vulnerability are privacy concerns and perceived risk. The factors of transparency, perceived control over location data and service reliability, on the other hand, are signals that can mitigate uncertainty and foster trust. This can then be linked to the perceived usefulness and acceptance intention (trust).

The conceptual study is about developing a framework to build user trust and privacy in location-based mobile navigation services. It merges these three theories (TAM, Privacy Calculus Theory, and Trust Theory) and puts forward eleven propositions that can be empirically tested in the future. The framework makes three contributions. It is not just privacy and trust added to TAM, but also considers privacy risk factors as distinct from trust-building factors. Second, it redirects attention away from the hypothetical boundary of data vulnerability and toward providers' promises and technology acceptance attitudes. Third, it is constrained by the framework, as it is only a consumer navigation service that relies on users to repeatedly or continuously reveal their location—thereby creating a lack of empirical evidence for the framework's validity.

The remainder of the paper is organized as follows. Section 2 – literature review is important and has identified a gap in the literature. In section 3, the conceptual research design, the literature selection process, the construct selection, and the theory integration and proposition development process are explained. The conceptual framework and research propositions are given in Section 4. In Section 5, the theoretical importance, the tentative practical implications, and the boundaries of the application are discussed. The constraints of this study are discussed in Section 6, future research directions are given in Section 7, and Section 8 concludes this paper.

2. Literature Review/Critical Synthesis

2.1. Location-Based Mobile Navigation Services

Location-based mobile navigation services are a niche subset of digital services that provide opportunities to make mobility decisions, estimate time of arrival, access real-time navigation information, and search for routes, relying on positioning, digital maps, traffic information, and user inputs. In the case of navigation services, location information is needed or recent; with other applications, it is not essential. Therefore, use of the service is contingent on sharing location information.

Past mobile service acceptability studies have emphasized value, ease of use, trust, and circumstances for adoption [22]. The same factors (privacy concern, personal innovativeness, perceived value, and perceived trust) were also found in studies on location-based services [23] and [24]. According to more recent studies in navigation research [19]-[21], users' attitudes toward the service quality attributes of reliability, usefulness, ease of use, and trust can also affect users' intention to reuse or accept the service. These studies are mainly oriented toward navigation performance or system acceptance, without a clear privacy–trust mechanism.

There is a need for both technical performance and data stewardship in the navigation context. While a provider may implement excellent privacy measures, if the routing, traffic data, or location data is incorrect, the provider will not convince users to trust those measures. If a provider has good privacy protections but either users do not trust the provider because the route information or traffic is unreliable, or the provider does not provide sufficient information to make users feel comfortable, then the provider loses users' trust. However, when users think that too much or too little location information is being disclosed, or that they are using location without explanation, it can be rejected as lacking technological soundness. Both of these aspects should be taken into account by a context-specific acceptance framework.

2.2. Technology Acceptance Perspective

TAM states that the two most important beliefs related to technology acceptance are perceived usefulness

and perceived ease of use [6]. Perceived usefulness is defined as the user's beliefs about how useful he or she expects a service to be, and perceived ease of use is defined as the user's beliefs about how easy he or she expects a service to be to use. Usefulness in a mobile navigation system can manifest as time savings, optimized routes, congestion avoidance, and reduced travel uncertainty. Easy-to-understand maps, easy route entry, clear voice directions, and manageable settings can improve usability.

According to UTAUT and UTAUT2, there are other factors, including performance expectancy, effort expectancy, social influence, facilitating conditions, hedonic motivation, price value, and habit, which can be added to the adoption view. The present model does not fully represent the UTAUT model, and these extensions are only valid for technologies in the consumer market. It is specifically designed to highlight the connections among privacy risk mechanisms, trust-building mechanisms, and the basic TAM pathway.

TAM is thus still considered the focal acceptance-outcome model. It is postulated that perceived ease of use affects perceived usefulness, which in turn affects intention to accept. This pathway is extended by placing trust before perceived usefulness and intention to accept the technology in this framework.

2.3. Three conceptions of privacy – Privacy Calculus, Privacy Concern, and Perceived Risk

The general trust users lack regarding the collection, storage, analysis, disclosure, and reuse of their personal data is known as "privacy concern" [25]. The above are especially relevant to Location-Based Navigation, where accurate positioning data can be utilized to provide information for routine and sensitive areas, and can be processed continuously or in the background. As opposed to "actual risk", perceived risk is more specific and is the expectation of a negative event. In this instance, the expectation is that tracking is taking place, that they are being profiled, that their data is being shared with third parties (or that they are losing control).

According to the Privacy Calculus Theory, when a person decides to disclose their personal information, they would consider the cost in terms of their privacy loss [9], [10]. Users are willing to disclose as long as the benefits of disclosure (in the context of location-based services: accuracy, personalization, and/or convenience in finding information) are perceived to outweigh the risks. However, not all the reasoning is sound and entirely logical. Positive conflicting beliefs, routine, and lack of information are also factors affecting privacy decisions [26]–[30], as is context.

The continued importance of privacy assessments is demonstrated in recent studies. Users' motivation to protect their privacy affects their reactions to place-based mobile applications [31], and privacy concerns remain relevant in place-based advertising applications [32]. Research on contact- or location-tracing applications has found that privacy concerns, perceived benefits, institutional trust, and situational factors can all be equally important in determining adoption of such applications [26]–[29]. This corroborates the results of the present study and suggests that privacy concerns and perceived risk should be taken into account, but that they do not necessarily have direct impacts and are not "settled" in all situations.

The framework therefore distinguishes privacy concern from perceived risk privacy and perceived risk. Increase perceived risk by introducing privacy concern as a general concern – makes potential negative consequences more salient. Both constructs are suggested to decrease trust by increasing users' vulnerability and uncertainty about the service provider.

2.4. Trust in Privacy-Sensitive Digital Services

Trust is the intention to rely on another person in an uncertain, vulnerable situation. For technology-mediated services, there are generally implicit assumptions of competence, integrity and benevolence that are supposed to be trusted [11], [12]. Mobile navigation competence can be described as the ability to provide accurate and timely instructions; integrity and benevolence are properties of an appropriate use of the user's localization information.

Trust is conceptually distinct from perceived risk. Reliance is acceptable when there is uncertainty because of positive beliefs and perceived negative consequences; this is trust. The two constructs are very closely related but not alternatives or other units. Users' privacy concerns and risk perceptions can erode trust, whereas tangible indicators of provider accountability, provider control, and technical reliability can positively impact trust.

Trust has been found to affect the acceptance of privacy-sensitive technologies across various settings, including online [33], [34], health apps [35], [36], social media [37], biometrics and public data [38], and the health industry. Notably, studies on trust adopt different perspectives and consider it either a direct antecedent, a mechanism, or an outcome of privacy and assurance beliefs. Once again, this change highlights the need to explicitly state that there is a role for trust as a cause in this model and not to use theory.

The suggested model places trust as a precondition for both user acceptance intention and perceived utility. It is not positioned as a mediator between acceptance intention and perceived usefulness but as an intermediary factor between perceived usefulness and intention. This is a conceptual study and does not seek to test the possibility of an indirect path in the sequence trust – perceived usefulness – user acceptance intention.

2.5. Transparency, Perceived Control, Data Governance, and Service Reliability

Transparency relates to the amount of information that users are provided with regarding location data practices, which is clear, accessible, and comprehensible. This may include information on the type and purpose of the information gathered, how long it is retained, whether it is used in conjunction with other information, whether it is transferred to a third party, and users' rights. Transparency increases the accessibility of information and can help the provider be seen as having integrity; however, transparency is not understanding or trust.

Perceived control over location information is an individual's belief in their ability to decide whether to share it. May include consent to location (precise or imprecise), restricting background tracking, deleting location history, revoking consent, and restricting sharing with third parties. Helplessness can be decreased and disclosure decisions more informed with meaningful control and institutional privacy assurances [39]–[42]

In this context, privacy policies or data-usage policies, as governance mechanisms to underpin transparency and perceived control, are viewed as part of privacy rather than as a separate construct. A policy is understandable, specific, accessible, and timely; it then contributes to transparency. Only contributes to a sense of control when linked to options and relevant privacy settings [42]. Data-governance assurance is a concept that could be studied as a standalone or a higher-order concept in the future.

Service reliability is the consistency of navigation; the service should be correct, on time, and available throughout the service. This includes the quality of routing service, positioning stability, traffic information, the accuracy of estimated arrival time, and the availability of services. Reliability is a description of the observable evidence of competence. So, it does not need to be a privacy mechanism, but it can be used to build trust [16], [24].

Research in the fields of privacy-friendly location-based services [40]–[42], informed consent [40], [43], transparency–control mechanisms [44]–[45], personal data categories [45], and geo-profile awareness [44] supports communication and user agency in governance. However, it is not a universal rule that relationships will be positive. Over-disclosure – or over-complexity of disclosure – can increase awareness of the risk, and complex controls that people do not understand can be delusions of agency. So, the suggested effects remain only speculative and must be proven through empirical testing.

2.6. Mobile-App Continuance and the Need for Contextual Boundaries

The intention to use the mobile application does not guarantee continuous use, and apps are often used multiple times. The literature on mobile applications has been surveyed, and it turns out that the customer experience, service quality, value, trust, and continuance mechanisms are emphasized [46], [47]. Navigation services do not just depend on context; they are also highly routinized, meaning that users might use the service when they are in a hurry, in an unfamiliar place, or in a car.

The current model focused on initial or general user acceptance intention rather than satisfaction, habit, or continuance intention. This boundary allows maintaining parsimony without combining the pre-adoption and post-adoption constructs or separating them. The evaluation of proposed acceptance relationships may be considered in the future for repeated use of the model.

2.7. Critical Synthesis and Research Gap

The literature reviewed shows that factors such as technology acceptance beliefs, privacy concerns, perceived risk, trust, transparency, control, and service quality will impact decisions regarding digital services. The evidence needs to be disjointed and incomplete, however. Performance and effort evaluations are typically highlighted in technology-acceptance studies, costs and benefits of disclosure have been highlighted in privacy-calculus studies, and vulnerability acceptance has been highlighted in trust studies. These streams are parallel but are generally considered separate in the modelling process and modelled independently, without explicit mention of each stream's function.

The second one is related to the context. Much of the historical data relates to e-commerce, social networks, location-based advertising, health apps, contact tracing, location-based services, and even MaaS. Although helpful beginnings, these studies are limited in that they do not reflect the two-way aspect of consumer navigation: both providing directions and listening to disclosures, as well as the treatment of a revisited location.

Thirdly, there is the causal organization. Not all previous models differentiate constructs that make vulnerability and mechanisms that can help decrease uncertainty. Negative assessments include potential harm, privacy concerns, and perceived risk. Signals of trust can be offered by the service provider or the service itself, including transparency, perceived control, and service reliability. Being able to differentiate these groups will help explain the relationship between trust and TAM with respect to privacy and service beliefs.

What has not been studied is not that privacy, trust, or technology acceptance have never been studied, or even that technology acceptance has never been studied, but that privacy, trust, or technology acceptance have not been sufficiently integrated into a coherent, context-specific framework for consumer mobile navigation services. What remains to be answered is how to integrate such well-known objects into a unified causal space for

Table 1. Critical comparison of relevant research streams.

Research stream	Typical context	Primary emphasis	Representative evidence	Limitation addressed by this study
Technology acceptance	General digital technologies	Usefulness, ease, performance, and effort	[6]–[8]	Limited explanation of vulnerability arising from repeated location disclosure
Privacy calculus	E-commerce, disclosure, and location-based services	Benefits versus privacy costs	[9], [10], [26]–[30]	Often weakly connected to navigation performance and service reliability
Trust-based adoption	E-commerce, digital platforms, and privacy-sensitive applications	Competence, integrity, benevolence, and willingness to rely	[11], [12], [33]–[38]	The causal position of trust varies across models and contexts
Location-based service privacy	Advertising, social networking, contact tracing, and MaaS	Privacy concern, risk, disclosure, control, and institutional trust	[13]–[18], [26]–[29], [31], [32]	Findings may not transfer directly to consumer navigation
Mobile navigation and service quality	Navigation systems and mobile navigation applications	Usefulness, ease of use, reliability, trust, service quality, and reuse	[19]–[21]	Privacy governance and trust-building mechanisms are often secondary
Proposed framework	Voluntary consumer mobile navigation	Privacy-risk factors, trust-building factors, trust, and the TAM pathway	Present conceptual synthesis	Conceptual only; requires future empirical validation

the space-integrated mobile navigation service, as it relates to a mobile user's environment. A framework is proposed in this paper that could solve the problem of trust as a theoretical link among the privacy risk factors, trust-building factors, and the TAM acceptance pathway. Critical comparisons are shown in Table 1.

3. Methodology

3.1. Conceptual Research Design

In this paper, the approach is a structured conceptual model development approach. The objectives are to achieve complementary integration of theory, identify constructs suitable to the context, identify relationships among the constructs, and propose directions for future empirical research. Design should be explicitly expressed when conducting conceptual research, and it is important to justify, on the one hand, the role of each of the theories, and on the other hand, that the synthesis that is proposed brings a value of explanation [48]-[50].

This paper is conceptual, not empirical or a formal systematic review. No statistical test of causal relationship was done, and the main data were not collected. A structured literature search was conducted to guide theory development, proposition identification, and critical synthesis.

3.2. Literature Identification and Selection Strategy.

The following search platforms, mostly interdisciplinary academic search databases, are used for the literature search: ScienceDirect, SpringerLink, IEEE Xplore, ACM Digital Library, Taylor & Francis Online, and Oxford Academic. The principal literature window was defined as January 2020 to July 2026 to prioritize recent research. However, seminal studies were retained when necessary to establish the theoretical foundations of TAM, Privacy Calculus Theory, information privacy, and Trust Theory.

Search for application-context terms, such as "mobile navigation", "navigation app", "location-based service", "location tracking" and "Mobility-as-a-Service", as well as privacy/trust terms, including "privacy concern", "perceived risk", "trust", "transparency", "perceived control", "privacy policy", "data governance" and "service reliability", and for acceptance terms, including "acceptance", "adoption", "behavioral intention", "continuance" and "reuse". The development of the search strings was customized for each source. Additionally, forward and backward citation searches were conducted to identify seminal works and linked contemporary studies. Rather than calculating actual effects, the literature selection was done for theoretical synthesis. As a result, the selection process was iterative and concept-driven, focusing on identifying relevant constructs, theoretical connections, and corroborating evidence to develop a framework. This method aligns with standards for conducting thorough conceptual literature evaluations that prioritize transparent searching, critical synthesis, and theory development [51], [52]. An outline of the literature identification and selection process is given in Figure 1.

3.3. Inclusion and Exclusion Criteria

Studies were considered if they: (1) contained a study on acceptance or adoption or disclosure or use or reuse or continuance, (2) included a study of a "Location Based, Mobile, Mobility or other Privacy Sensitive Digital Service", (3) included a study of at least one of the constructs related to privacy, risk, trust, transparency, control, reliability, usefulness, and ease of use and (4) had a clear conceptual or empirical explanation of the relationship studied.

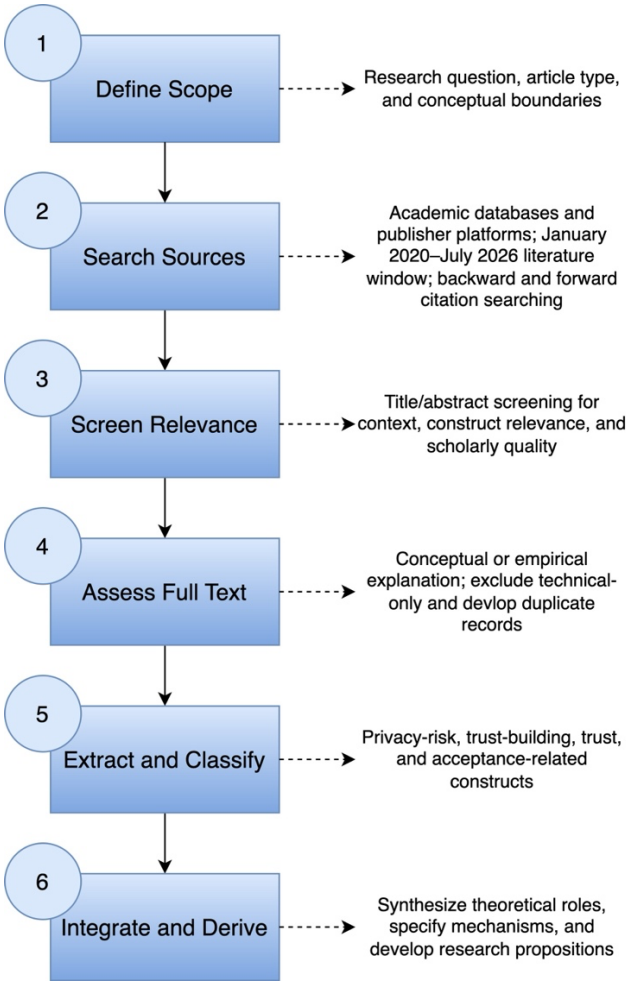

Figure 1. Literature identification and selection strategy.

Research papers not included were those that did not consider a construct from the user's perspective, focused exclusively on positioning algorithms, technical security measures, or organizational constructs, were not conceptually/methodologically detailed enough, or were previously published. Regardless of the year of publication, seminal theoretical papers were kept when necessary to lay the groundwork for TAM, Privacy Calculus Theory, information privacy, and Trust Theory.

3.4. Construct Selection and Exclusion

The evaluation and comparison of the candidate constructs were based on the following attributes: theoretical relevance, applicability to repeated location disclosure, conceptual distinctiveness, support for multiple research streams, and model parsimony. The evaluations of privacy concern and perceived risk were kept as vulnerability-related evaluations. The trust-building attributes that were retained were transparency, perceived control over location data, and service reliability. The relationship between privacy-related assessments, service-related attributes, and technology acceptance attitudes was maintained as trust. User Acceptance, Perceived Utility, and Perceived Usability: Since they clarify users' acceptance choices and intentions, items were retained from TAM.

Those not included in the core framework were social influence, facilitating conditions, habit, hedonic motivation, price value, satisfaction, provider reputation and personal innovativeness and privacy awareness. Such constructs might be suitable but are outside the primary theme of the model, namely the privacy-risk, trust-building, and TAM constructs. They can be used as a control, a mediator, or a continuation in future empirical studies.

3.5. Theory Integration

The knowledge in the framework is a logic of theory synthesis, in which the various theories play different roles in the explanation. TAM explains the relationships among perceived ease of use [19], perceived usefulness, and acceptance intention, addressing the acceptance-outcome relationship [6]. According to the Privacy Calculus Theory [9], [10], repeated disclosure of a site results in the development of an evaluation of potential benefits and potential privacy costs. Trust Theory: Users will be willing to be vulnerable if they hold positive beliefs about providers' competence, integrity, benevolence, and reliability [11], [12].

These theories are complementary and explain different aspects of user decision-making. Privacy Calculus Theory explains how users evaluate potential benefits and privacy risks associated with location-data disclosure. Trust Theory explains how users decide whether they can rely on service providers under conditions of uncertainty. TAM explains how usefulness and ease-of-use beliefs influence acceptance intention. Therefore, the proposed framework integrates privacy evaluation, trust formation, and technology acceptance into a unified conceptual structure. Trust serves as the theoretical bridge connecting privacy and service-related factors with acceptance outcomes, as illustrated in Figure 2 and Table 2 explain the unique contribution of each theoretical foundation.

3.6. Proposition Development

All the propositions were developed in 5 stages: identification of the theoretical foundation of the proposition, identification of the predictor constructs, identification of the outcome constructs, incorporation of the mechanism within the context of mobile navigation, and a literature review that supports or challenges the mechanism. Then each relationship was clearly specified.

The effects are not substantiated; rather, the propositions are hypothetical predictions. No primary data or statistical tests were used. Hence, the research directions, indirect pathways, implications for practice, and boundary conditions presented here need to be confirmed through future empirical studies.

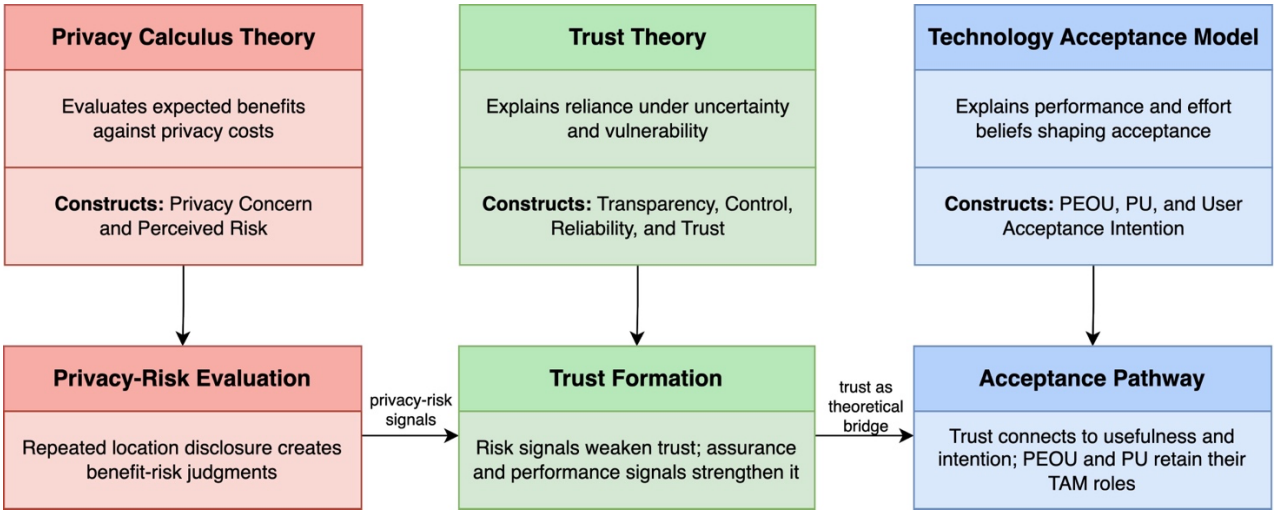

Figure 2. Theory integration logic.

Table 2. Unique contribution of each theoretical foundation.

Theory	Unique explanatory role	Constructs and pathways retained in the framework
Privacy Calculus Theory	Explains how users evaluate expected service benefits against privacy costs when location disclosure is required [9], [10], [26]–[30].	Privacy Concern → Perceived Risk; privacy-risk evaluations as antecedents of Trust
Trust Theory	Explains willingness to rely on a provider under uncertainty and vulnerability [11], [12], [33], [34].	Transparency, Perceived Control, and Service Reliability → Trust; Trust → Perceived Usefulness and Acceptance Intention
Technology Acceptance Model	Explains how performance and effort beliefs shape technology acceptance [6]–[8].	Perceived Ease of Use → Perceived Usefulness and Acceptance Intention; Perceived Usefulness → Acceptance Intention

4. Conceptual Framework and Proposition Development

4.1. Proposed Framework

The proposed framework comprises nine constructs, broken down into privacy-risk factors, trust-building factors, a connecting trust construct, and acceptance factors. The privacy-risk group comprises privacy concern and perceived risk. The trust-building group comprises transparency, perceived control over location data, and service reliability. The factors that make up the acceptance group of the TAM are perceived usefulness, perceived ease of use, and user acceptance intention.

The framework proposes that privacy concern and perceived risk reduce trust, whereas transparency, perceived control, and service reliability strengthen trust. Trust subsequently increases perceived usefulness and user acceptance intention. Perceived ease of use increases perceived usefulness and user acceptance intention, and perceived usefulness increases user acceptance intention. The sequence trust → perceived usefulness → user acceptance intention indicates a potential indirect pathway, but no mediation claim is made because the model has not been empirically tested. Figure 3 presents the framework and the expected directions of P1–P11.

4.2. Privacy Concern, Perceived Risk and Trust.

Privacy is the primary concern regarding the collection, storage, analysis, sharing, and secondary use of information about their locations. Perceived risk – Risk and consequence are more context-specific. Those more privacy-conscious feel more strongly than others about continuous tracking, background access, location history, and the sharing of that with third parties, getting the better of mobile navigation. Thus, privacy concerns are more likely to be a source of perceived risk, as concluded in [9], [10], [25], rather than the reverse.

P1: *Privacy concern positively influences perceived risk in location-based mobile navigation services.*

The service provider's trust in the service user requires several assumptions that the service provider will act competently and responsibly – which is difficult for the service user to see. High privacy concern indicates uncertainty about whether providers will act in users' interests regarding users' interests. Therefore, if the user is concerned about excessive data collection, they are less willing to use the provider when there is excessive secondary or unauthorized use [13], [16], [17].

P2: *Privacy concern negatively influences trust in location-based mobile navigation services.*

Trust is about being vulnerable; perceived risk is about being salient with respect to the outcomes potentially associated with that vulnerability. Users may be less inclined to depend on the provider if they anticipate

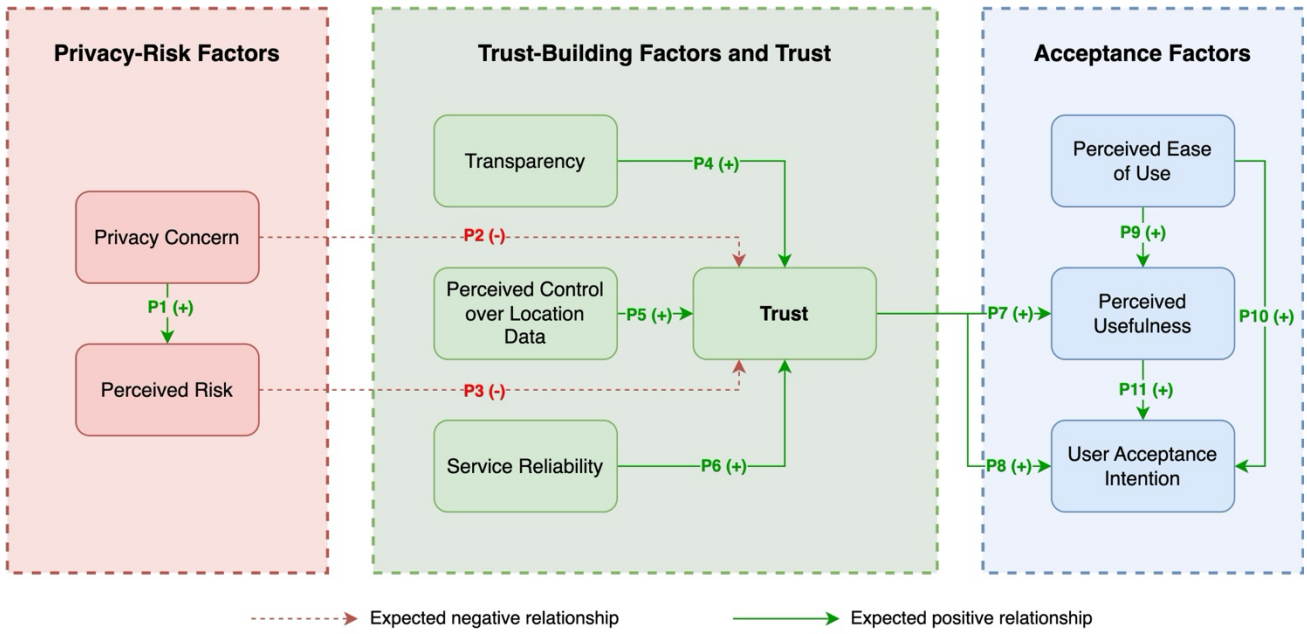

Figure 3. Proposal of a new user acceptance model taking into account trust and privacy.

tracking, profiling, data leaks, or a loss of control. Therefore, it can be assumed that the riskier the perception, the less trust there will be [9]–[12].

P3: *Perceived risk negatively influences trust in location-based mobile navigation services.*

4.3. Transparency, Perceived Control, Service Reliability, and Trust.

Information asymmetry can be reduced by making information transparent to users, e.g., informing them what information is being collected. For this purpose, for how long, and whether it can be shared. Clarity and straightforwardness can also be characteristics of responsibility and integrity. Most data use and applications are behind the scenes and invisible to the user, and mechanisms to verify the provider's trustworthiness are useful [39]–[41].

P4: *Transparency positively influences trust in location-based mobile navigation services*

Perceived control relates to users' sense of control over the collection of their location data and its use. Removing some of the complexities of exposure can help ease the feeling of loss of control with tips such as disabling background tracking, using approximate location, clearing the location history, revoking permission and limiting sharing. Effective control seems crucial to improving the user's sense of control over the provider [10], [39], [42].

P5: *Perceived control over location data positively influences trust in location-based mobile navigation services.*

However, responsible data handling also goes hand in hand with confirmed technical capabilities to win consumer confidence in a mobile navigation provider. The observable evidence of the provider's ability to perform the promised functions relates to the accuracy of the routes provided, the stability of position, the timely provision of traffic information, service availability, and the reliability of the estimated arrival time. Thus, it can be expected that Consistent performance is therefore expected to support competence-based trust. to be competent [16], [19].

P6: *Service reliability positively influences trust in location-based mobile navigation services.*

4.4. The three components of trust, perceived usefulness, and user acceptance intention.

Workability (ease of use) is an integral component of the perceived usefulness that stems from the credibility and real actions/options offered for the information and recommendations the service offers. Even the most sophisticated navigation service might be deemed less effective if the user lacks confidence in the service and/or its provider. Thus, trust can be applied to enhance usefulness assessments by making navigation output more reliable and to build trust in navigation, thereby enhancing valued travel benefits [12], [20].

P7: *Trust positively influences the perceived usefulness of location-based mobile navigation services.*

Place-based mobile navigation requires users to be vulnerable, grant access to their location data, and trust the navigation provider. Trust minimizes uncertainty about data usage and enhances the service's effectiveness and reliability. It is assumed that users are more likely to accept results based on their perceptions of the provider's competence, honesty, and responsibility [17], [18], [33].

P8: *Trust positively influences user acceptance intention toward location-based mobile navigation services.*

Table 3. Summary of Research Propositions.

Proposition	Proposed Relationship	Expected Direction	Theoretical basis and indicative evidence
P1	Privacy Concern → Perceived Risk	Positive	Privacy-calculus and information-privacy reasoning [9], [10], [25]
P2	Privacy Concern → Trust	Negative	Privacy vulnerability and trusting beliefs [13], [16], [17]
P3	Perceived Risk → Trust	Negative	Risk and willingness to accept vulnerability [9]–[12]
P4	Transparency → Trust	Positive	Information asymmetry, integrity signals, and institutional assurances [39]–[41]
P5	Perceived Control → Trust	Positive	User agency and privacy control [10], [39], [42]
P6	Service Reliability → Trust	Positive	Competence-based trust and navigation-service quality [16], [19]
P7	Trust → Perceived Usefulness	Positive	Credibility and usefulness of service outputs [12], [20]
P8	Trust → User Acceptance Intention	Positive	Reliance under uncertainty [17], [18], [33]
P9	Perceived Ease of Use → Perceived Usefulness	Positive	Technology Acceptance Model [6]–[8]
P10	Perceived Ease of Use → User Acceptance Intention	Positive	Technology Acceptance Model [6]–[8]
P11	Perceived Usefulness → User Acceptance Intention	Positive	Technology Acceptance Model and navigation evidence [6], [19], [20]

4.5. Perceived ease of use, perceived usefulness and the intention to use.

If it is easy to learn and use, less cognitive and procedural effort will be required to learn and use a navigation service. Besides that, its intuitive route entry, guidance, and map, along with user-friendly privacy settings, allow users to enjoy the benefits of navigation more efficiently. Therefore, perceived ease of use is likely to affect perceived usefulness positively [6]–[8].

P9: *Perceived ease of use positively influences the perceived usefulness of location-based mobile navigation services.*

Regardless of how beneficial the service's features are, it can be off-putting if its interfaces are complicated, its permissions are unclear, or the route selection process is tricky. On the other hand, an easy-to-learn-and-use application reduces effort barriers. Therefore, it can be expected that perceived ease of use will also positively influence the intention to accept the software [6]–[8].

P10: *Perceived ease of use positively influences user acceptance intention toward location-based mobile navigation services.*

The greater the users' perception that the navigation service could benefit their travel route selection, reduce travel uncertainty, provide timely traffic information, and enable smart travel decisions, the more they accept the navigation service. Perceived usefulness is the value of the service from the user's perspective, and it is hypothesized that increasing the user's intention to accept the service is possible [6], [19], [20]. Table 3 presents a summary of the proposed research propositions.

P11: *Perceived usefulness positively influences user acceptance intention toward location-based mobile navigation services.*

5. Discussion

5.1. Theoretical Contributions

The most significant aspect of the framework, in terms of theory, is that it establishes trust as the link between privacy and service-evaluation beliefs and between existing technology-acceptance beliefs. A related but different notion of privacy concern is vulnerability, which is perceived risk. Integrity, user independence, and ability encompass transparency, perceived control, and service reliability. This separation can lead not only to potential distrust of a navigation provider by the user but also to potential trust-building.

The framework is not intended to replace the TAM but rather to extend it. However, there is still perceived usefulness – users must see whether navigation services positively affect mobility decisions – and perceived ease of use, which measures whether the navigation services are easy to use and require little effort. However, for services, which are likely to be location-based, the effort beliefs (and service performance) may be insufficient. Trust

can affect users' beliefs about the accuracy of navigation information and about being vulnerable when using it.

The integration also makes clear the role of each theory. The Theory of Privacy Calculus is related to evaluating privacy; the Theory of Trust is related to reliance on trust in vulnerable situations; and the Theory of Technology Acceptance is related to technology acceptance. Sequential logic helps to solve the issue of the combination of known elements without a theoretical basis.

5.2. Provisional Practical Implications

Due to the lack of empirical testing and practical implications, propositions need to be considered with caution. To gain trust, the navigation-service provider should explicitly state the provider's policy on how the location information is used, give the user the option to either grant or refuse access to the location information, and give an accurate (and trusted) navigation.

Transparency should not be limited to publishing a lengthy privacy policy. transparency should be easier to understand. Should include brief explanations regarding the use, retention, sharing and user decisions of data when appropriate. Similarly, the feeling of control should be communicated realistically, not in a way users cannot understand. Reliability work should take into consideration the reliability of the service (information) and the reliability of the technical performance. These implications are tentative, as the proposed relationships have yet to be tested with users and in behavioral outcomes.

5.3. Boundary Conditions

The approach is limited to consumer-facing, voluntary mobile navigation services that repeatedly or continuously disclose location that is consumer-facing, in services for mobile navigation. It can be multiple, for example, in some governmental systems, the navigation system in an organization, in emergency response systems, in autonomous vehicles, or in other contexts where there is no choice for the users.

Measures of relationship-proposed strength may vary across different cultures, privacy regulations, provider reputation, operating-system governance, experience, task urgency, and privacy awareness. Another aspect of trust could be with public institutions, service providers, platforms, and applications. These conditions need to be indicated in empirical applications of the model.

6. Limitations

There are few limitations to this study. The first is that it is conceptual; there is no empirical test of any relationship. Secondly, the selected construct types align with the literature reviewed and are linked to the included constructs, but may not account for other factors such as social influence, habit, satisfaction, facilitating conditions, provider reputation, and privacy awareness. Thirdly, the model is intended to guide use rather than predict permission decisions or technology use/continued use. Fourthly, there is no modelling of regulatory and/or platform governance, service provider(s) culture and reputation, and/or prior experience. Finally, the causal ordering proposed here is theoretically defensible, and other orderings might be defensible.

7. Future Research

Data from mobile navigation application users should be used in future testing of the proposed measurement and structural model. It is recommended to test the validity of the measures and establish the direction, strength, and significance of the hypothesized relationships by using SEM (covariance-based) and PLS-SEM.

Two or more competing models are to be compared. The direct path from perceived risk to intention to use, the indirect path from trust to intention to use, and the indirect path from privacy concern to trust via perceived risk. These analyses should be empirical, not assumed based on a conceptual framework.

Future longitudinal and behavioral studies are needed to determine whether there is a correlation between intention to use and setting, sharing location, adoption, and continued use. The different regulatory environments, platforms, providers, age groups, levels of privacy awareness, and previous navigation experience/digital literacy can be explored using cross-cultural and multi-group analyses. Data-governance assurance can also be investigated further as a higher-order construct, an independent antecedent, or a moderator in future studies.

8. Conclusion

This conceptual study provides a theoretical framework grounded in trust and privacy to explain users' intention to accept location-based mobile navigation services. The framework combines three theories: TAM, Privacy Calculus Theory, and Trust Theory, which take into consideration both the functional value of navigation and vulnerability caused by repeated disclosure of location information. It suggests that privacy concerns and perceived risk reduce trust, while transparency, perceived control over location data, and service reliability increase trust. Trust is seen as an antecedent of perceived usefulness and user acceptance intention; perceived ease of use and perceived usefulness are kept in their proper place in the technology-acceptance pathway.

The framework adds value by separating privacy-risk assessments from trust-building mechanisms and clarifying how these assessments and mechanisms might tie into acceptance beliefs in a mobile-navigation context. The suggested relationships are conceptual and not supported by empirical evidence. The propositions presented

in this paper should be tested in the future using survey and behavioral data, as well as by investigating the strength of the propositions across platforms, providers, user groups, cultures, and regulatory environments.

9. Abbreviations

Abbreviation	Meaning
MaaS	Mobility as a Service
PEOU	Perceived Ease of Use
PU	Perceived Usefulness
TAM	Technology Acceptance Model
UAI	User Acceptance Intention
UTAUT	Unified Theory of Acceptance and Use of Technology
UTAUT2	Unified Theory of Acceptance and Use of Technology

10. Declarations

10.1. Author Contributions

Atta Ur Rahman: Conceptualization, Methodology, Investigation, Writing - Original Draft, Writing - Review & Editing; **Fuyang Ke:** Supervision, Methodology, Validation, Writing - Review & Editing; **Muhammad Raza:** Validation, Writing - Review & Editing.

10.2. Institutional Review Board Statement

Not applicable.

10.3. Informed Consent Statement

Not applicable.

10.4. Data Availability Statement

No new data were created or analyzed in this study. This paper is a conceptual study based on a structured review and synthesis of previously published literature.

10.5. Acknowledgment

Not applicable.

10.6. Conflicts of Interest

The authors declare no conflicts of interest.

11. References

[1] J. W. Kim, K. Edemacu, and B. Jang, "Privacy-preserving mechanisms for location privacy in mobile crowdsensing: A survey," *J. Netw. Comput. Appl.*, vol. 200, Art. no. 103315, Apr. 2022. https://doi.org/10.1016/j.jnca.2021.103315..

[2] G. Qiu, G. Tang, C. Li, L. Luo, D. Guo, and Y. Shen, "Differentiated location privacy protection in mobile communication services: A survey from the semantic perception perspective," *ACM Comput. Surv.*, vol. 56, no. 3, Art. no. 60, pp. 1–36, Mar. 2024. https://doi.org/10.1145/3617589.

[3] S. Heitmann, A. Pagotto, and C. Kray, "Approximate vs. precise location in popular location-based services," *Journal of Location Based Services*, vol. 19, no. 1, pp. 1–42, 2025. https://doi.org/10.1080/17489725.2024.2310006.

[4] S. Özdal Oktay, S. Heitmann, and C. Kray, "Linking location privacy, digital sovereignty and location-based services: A meta review," *Journal of Location Based Services*, vol. 18, no. 1, pp. 1–52, 2024. https://doi.org/10.1080/17489725.2023.2239180.

[5] Z. Garroussi, A. Legrain, S. Gambs, V. Gautrais, and B. Sansò, "A systematic review of data privacy in Mobility as a Service (MaaS)," *Transportation Research Interdisciplinary Perspectives*, vol. 31, art. 101254, 2025. https://doi.org/10.1016/j.trip.2024.101254.

[6] Y. Ge, H. Qi, and W. Qu, "The factors impacting the use of navigation systems: A study based on the technology acceptance model," *Transp. Res. Part F Traffic Psychol. Behav.*, vol. 93,

pp. 106–117, Feb. 2023. https://doi.org/10.1016/j.trf.2023.01.005.

[7] Z. Kenesei, L. Kökény, K. Ásványi, and M. Jászberényi, "The central role of trust and perceived risk in the acceptance of autonomous vehicles in an integrated UTAUT model," *Eur. Transp. Res. Rev.*, vol. 17, Art. no. 8, 2025. https://doi.org/10.1186/s12544-024-00681-x.

[8] C. Varela-Neira and A. Hilal, "A UTAUT2 approach to understand intention to use mobile banking by non-users and intention to continue by users," *J. Financ. Serv. Mark.*, vol. 31, Art. no. 23, Feb. 2026. https://doi.org/10.1057/s41264-026-00350-1.

[9] B. Binzer, J. Kendziorra, A.-K. Witte, and T. J. Winkler, "Trust in public and private providers of health apps and usage intentions: A sectoral privacy calculus and control perspective," *Bus. Inf. Syst. Eng.*, vol. 66, pp. 273–297, Jun. 2024. https://doi.org/10.1007/s12599-024-00869-4.

[10] S. Cerf, B. Robu, N. Marchand, and S. Bouchenak, "Privacy protection control for mobile apps users," *Control Eng. Pract.*, vol. 134, Art. no. 105456, May 2023. https://doi.org/10.1016/j.conengprac.2023.105456.

[11] J.-G. Martínez-Navalón, M. Fernández-Fernández, and F. P. Alberto, "Does privacy and ease of use influence user trust in digital banking applications in Spain and Portugal?," *Int. Entrep. Manag. J.*, vol. 19, no. 2, pp. 781–803, Jun. 2023. https://doi.org/10.1007/s11365-023-00839-4.

[12] J. M. Lopes, I. Massano-Cardoso, and L. Pedrosa, "The role of artificial intelligence in mobile banking: Decoding Portuguese consumers' perceptions and intentions to engage," *Future Bus. J.*, vol. 11, Art. no. 125, May 2025. https://doi.org/10.1186/s43093-025-00510-0.

[13] F. Bemmann and S. Mayer, "The impact of data privacy on users' smartphone app adoption decisions," *Proc. ACM Hum.-Comput. Interact.*, vol. 8, no. MHCI, Art. no. 278, pp. 1–23, Sep. 2024. https://doi.org/10.1145/3676525.

[14] Y. Ma, C. Sew, Z. Sarsenbayeva, J. Knibbe, and J. Goncalves, "Understanding users' perspectives on location privacy management on iPhones," *Proc. ACM Hum.-Comput. Interact.*, vol. 8, no. MHCI, Art. no. 282, pp. 1–25, Sep. 2024. https://doi.org/10.1145/3676529.

[15] Y. Jung, J. A. Bao, M. P. Norman, and S. S. Sundar, "Privacy concerns in mobile technology: Can interactivity reduce friction?," *Comput. Hum. Behav.*, vol. 162, Art. no. 108421, Jan. 2025. https://doi.org/10.1016/j.chb.2024.108421.

[16] A. H. Shoabjareh, M. Ghasri, T. Roberts, A. Lapworth, N. Dobos, and C. Boshuijzen-van Burken, "The role of trust and distrust in technology usage: An in-depth investigation of traffic information apps usage for mandatory and non-mandatory trips," *Travel Behav. Soc.*, vol. 37, Art. no. 100816, Oct. 2024. https://doi.org/10.1016/j.tbs.2024.100816.

[17] S. Huang, "Listening to users' personal privacy concerns: The implication of trust and privacy concerns on the user's adoption of a MaaS-pilot," *Case Studies on Transport Policy*, vol. 10, no. 4, pp. 2153–2164, 2022. https://doi.org/10.1016/j.cstp.2022.09.012.

[18] N. F. A. Budi et al., "Why do people want to use location-based applications for emergency situations? The extension of UTAUT perspectives," *Technology in Society*, vol. 65, art. 101480, 2021. https://doi.org/10.1016/j.techsoc.2020.101480.

[19] M. J. Bryant, S. J. Wilde, G. Coles, G. Sorwar, and V. Bui, "Mobile app usage and adoption through the lens of cognitive, affective and behavioral trust constructs," *International Journal of Human–Computer Interaction*, vol. 42, no. 5, pp. 3393–3417, 2026. https://doi.org/10.1080/10447318.2025.2531289.

[20] S. Hu, L. Rong, J. Han, D. Zhang, and W. Jiang, "The effects of interaction mode and individual differences on usability and user experience of mobile augmented reality navigation," *IEEE Access*, vol. 11, pp. 41783–41795, 2023. https://doi.org/10.1109/ACCESS.2023.3271522.

[21] L. Yang, Y. Bian, X. Zhao, X. Liu, and X. Yao, "Drivers' acceptance of mobile navigation applications: An extended technology acceptance model considering drivers' sense of direction, navigation application affinity and distraction perception," *International Journal of Human–Computer Studies*, vol. 145, art. 102507, 2021. https://doi.org/10.1016/j.ijhcs.2020.102507.

[22] G. Lu, S. Qu, and Y. Chen, "Understanding user experience for mobile applications: A systematic literature review," *Discover Appl. Sci.*, vol. 7, Art. no. 587, Jun. 2025. https://doi.org/10.1007/s42452-025-07170-3.

[23] Y. Ma, S. Zhang, D. Yang, Z. Sarsenbayeva, J. Knibbe, and J. Goncalves, "Raising awareness of location information vulnerabilities in social media photos using LLMs," in *Proc. CHI Conf. Human Factors Comput. Syst. (CHI '25)*, Yokohama, Japan, Apr. 2025, pp. 1–14. https://doi.org/10.1145/3706598.3714074.

[24] M. J. J. Gumasing, J. Y. M. Nazal, A. C. Rivera, J. R. E. Robles, and J. A.-F. C. Viray, "Exploring Gen Z adoption of Life360 technology: A study of usage patterns and perceptions," *Acta Psychol.*, vol. 259, Art. no. 105422, Sep. 2025. https://doi.org/10.1016/j.actpsy.2025.105422.

[25] J. Bartol, V. Vehovar, and A. Petrovčič, "Systematic review of survey scales measuring information privacy concerns on social network sites," *Telemat. Inform.*, vol. 85, Art. no. 102063, Nov. 2023. https://doi.org/10.1016/j.tele.2023.102063.

[26] F. Hassandoust, S. Akhlaghpour, and A. C. Johnston, "Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective," *Journal of the American Medical Informatics Association*, vol. 28, no. 3, pp. 463–471, 2021. https://doi.org/10.1093/jamia/ocaa240.

[27] G. Fox, T. Clohessy, L. van der Werff, P. Rosati, and T. Lynn, "Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications," *Computers in Human Behavior*, vol. 121, art. 106806, 2021. https://doi.org/10.1016/j.chb.2021.106806.

[28] M. Trkman, A. Popovič, and P. Trkman, "The roles of privacy concerns and trust in voluntary use of governmental proximity tracing applications," *Government Information Quarterly*, vol. 40, no. 1, art. 101787, 2023. https://doi.org/10.1016/j.giq.2022.101787.

[29] S. Ying, Y. Huang, L. Qian, and J. Song, "Privacy paradox for location tracking in mobile social networking apps: The perspectives of behavioral reasoning and regulatory focus," *Technological Forecasting and Social Change*, vol. 190, art. 122412, 2023. https://doi.org/10.1016/j.techfore.2023.122412.

[30] T. Fernandes and N. Pereira, "Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online?" *Telematics and Informatics*, vol. 65, art. 101717, 2021. https://doi.org/10.1016/j.tele.2021.101717.

[31] N. Rodríguez-Priego, L. Porcu, and P. J. Kitchen, "Sharing but caring: Location-based mobile applications and privacy protection motivation," *Journal of Business Research*, vol. 140, pp. 546–555, 2022. https://doi.org/10.1016/j.jbusres.2021.11.022.

[32] R. Aggarwal, S. Dhingra, and S. Mittal, "What reduces the privacy concerns of customers toward the use of location-based advertising? An empirical investigation," *Journal of Location Based Services*, vol. 18, no. 2, pp. 139–161, 2024. https://doi.org/10.1080/17489725.2023.2256701.

[33] T. D. Oesterreich, E. Anton, F. M. Hettler, and F. Teuteberg, "What drives individuals' trusting intention in digital platforms? An exploratory meta-analysis," *Management Review Quarterly*, vol. 75, pp. 3615–3667, 2025. https://doi.org/10.1007/s11301-024-00477-2.

[34] M. S. Frangopoulou, L. N. van der Laan, and W. Ebbers, "The privacy calculus in the context of novel health technology for diagnosing and tracking infectious diseases: The role of disease severity and technology's evidence base for effectiveness in adoption and voluntary health data-sharing," *Technol. Soc.*, vol. 78, Art. no. 102616, Sep. 2024. https://doi.org/10.1016/j.techsoc.2024.102616.

[35] M. S. Alzaidi and G. Agag, "The role of trust and privacy concerns in using social media for e-retail services: The moderating role of COVID-19," *Journal of Retailing and Consumer Services*, vol. 68, art. 103042, 2022. https://doi.org/10.1016/j.jretconser.2022.103042.

[36] D. Dhagarra, M. Goswami, and G. Kumar, "Impact of trust and privacy concerns on technology acceptance in healthcare: An Indian perspective," *International Journal of Medical Informatics*, vol. 141, art. 104164, 2020. https://doi.org/10.1016/j.ijmedinf.2020.104164.

[37] Y. Zhang, "Impact of perceived privacy and security in the TAM model: The perceived trust as the mediated factors," *International Journal of Information Management Data Insights*, vol. 4, no. 2, art. 100270, 2024. https://doi.org/10.1016/j.jjimei.2024.100270.

[38] J. Kim, D. Kim, and B. David-John, "The role of privacy concerns, perceived benefits, and trust in citizens' acceptance of street-view image collection by local planning agencies," *Cities*, vol. 154, art. 105339, 2024. https://doi.org/10.1016/j.cities.2024.105339.

[39] Y. Hu and H. K. Min, "Information transparency, privacy concerns, and customers' behavioral intentions regarding AI-powered hospitality robots: A situational awareness perspective," *J. Hosp. Tour. Manag.*, vol. 63, pp. 177–184, Jun. 2025. https://doi.org/10.1016/j.jhtm.2025.04.003.

[40] J. Dreyer, S. Heitmann, F. Erdmann, G. Bauer, and C. Kray, "'Informed' consent in popular location-based services and digital sovereignty," *Journal of Location Based Services*, vol. 16, no. 4, pp. 312–342, 2022. https://doi.org/10.1080/17489725.2021.2017495.

[41] J. Cloarec, C. Cadieu, and N. Alrabie, "Tracking technologies in eHealth: Revisiting the personalization–privacy paradox through the transparency-control framework,"

Technological Forecasting and Social Change, vol. 200, art. 123101, 2024. https://doi.org/10.1016/j.techfore.2023.123101.

[42] F. Bemmann, M. Windl, J. Erbe, S. Mayer, and H. Hussmann, "The influence of transparency and control on the willingness of data sharing in adaptive mobile apps," *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. MHCI, Art. no. 189, pp. 1–26, Sep. 2022. https://doi.org/10.1145/3546724.

[43] P. Mirzania, N. Balta-Ozkan, and L. Whitmarsh, "Improved convenience or a cyber security threat? Public acceptance of mobility-as-a-service in Great Britain," *Energy Res. Soc. Sci.*, vol. 127, Art. no. 104309, Sep. 2025. https://doi.org/10.1016/j.erss.2025.104309.

[44] F. S. Alrayes, A. I. Abdelmoty, and W. El-Geresy, "User profile visualisation for privacy awareness on Geo-Social Networks," *Journal of Location Based Services*, vol. 19, no. 1, pp. 43–77, 2025. https://doi.org/10.1080/17489725.2024.2399512.

[45] H. N. Chua, J. S. Ooi, and A. Herbland, "The effects of different personal data categories on information privacy concern and disclosure," *Computers & Security*, vol. 110, art. 102453, 2021. https://doi.org/10.1016/j.cose.2021.102453.

[46] L. Stocchi, N. Pourazad, N. Michaelidou, A. Tanusondjaja, and P. Harrigan, "Marketing research on mobile apps: Past, present and future," *Journal of the Academy of Marketing Science*, vol. 50, no. 2, pp. 195–225, 2022. https://doi.org/10.1007/s11747-021-00815-w.

[47] S. Veronika, M. S. W. Lee, B. Lang, and P. Putra, "A systematic review and future agenda on continuance intentions in mobile apps," *International Journal of Information Management Data Insights*, vol. 5, no. 2, art. 100352, 2025. https://doi.org/10.1016/j.jjimei.2025.100352.

[48] E. Jaakkola, "Designing conceptual articles: Four approaches," *AMS Review*, vol. 10, pp. 18–26, 2020. https://doi.org/10.1007/s13162-020-00161-0.

[49] K. Heinonen and T. Gruen, "Elevating conceptual research: Insights, approaches, and support," *AMS Review*, vol. 14, nos. 1–2, pp. 1–6, 2024. https://doi.org/10.1007/s13162-024-00283-9.

[50] W. M. Lim, "Theory and theory development: Guidelines for establishing theoretical gaps, foundations, contributions, and implications," *Journal of Business Research*, vol. 202, Art. no. 115745, Jan. 2026. https://doi.org/10.1016/j.jbusres.2025.115745.

[51] M. Gusenbauer and S. P. Gauster, "How to search for literature in systematic reviews and meta-analyses: A comprehensive step-by-step guide," *Technological Forecasting and Social Change*, vol. 212, Art. no. 123833, Mar. 2025. https://doi.org/10.1016/j.techfore.2024.123833.

[52] J. Paul, A. Merchant, Y. K. Dwivedi, and G. Rose, "Writing an impactful review article: What do we know and what do we need to know?" *Journal of Business Research*, vol. 133, pp. 337–340, 2021. https://doi.org/10.1016/j.jbusres.2021.05.005.