Understanding Users' Perspectives on Location Privacy Management on iPhones

YING MA, University of Melbourne, Australia
CHERIE SEW, University of Melbourne, Australia
ZHANNA SARSENBAYEVA, University of Sydney, Australia
JARROD KNIBBE, University of Queensland, Australia
JORGE GONCALVES, University of Melbourne, Australia

As the number of applications installed on smartphones continues to grow, the task of effectively managing location privacy has become increasingly complex. In this paper, we explore the factors that influence users' privacy-preserving intentions and contrast them with their actual behaviours. In addition, we compare location privacy concerns across different apps investigating the impact of app-specific features on the willingness to disclose location information. Our findings highlight significant challenges in privacy management due to privacy fatigue and perceived usability. Furthermore, participants raised the importance of more uniform standards regarding location privacy settings across various applications, calling for more detailed and interactive well-informed consent processes that highlight the risks instead of the benefits of disclosing location information. This research contributes important insights towards the development of more effective privacy settings that can foster increased user engagement in managing location privacy on smartphones.

CCS Concepts: • **Human-centered computing → Empirical studies in HCI**.

Additional Key Words and Phrases: location privacy, smartphones, iPhones, privacy management, privacy paradox, Twitter, Instagram, Yelp

ACM Reference Format:
Ying Ma, Cherie Sew, Zhanna Sarsenbayeva, Jarrod Knibbe, and Jorge Goncalves. 2024. Understanding Users' Perspectives on Location Privacy Management on iPhones. *Proc. ACM Hum.-Comput. Interact.* 8, MHCI, Article 282 (September 2024), 25 pages. https://doi.org/10.1145/3676529

1 Introduction

On average, a person now has more than 80 apps installed on their smartphone [11], a significant increase from the average of 20 apps reported in 2019 among U.S. users [64]. As the number of applications on a smartphone grows, the risk associated with the indiscriminate installation of untrustworthy apps becomes more pronounced [43]. In order to mitigate some of these risks, smartphone operating systems and app developers have introduced various features (e.g., privacy labels in iOS, the different granularity of privacy controls, nudge notifications, etc) [1] to better inform users about the type of data collected as well as manage the disclosure of their information. Previous

[1] Privacy control features for iOS 14 (https://www.apple.com/au/privacy/control/)

Authors' Contact Information: Ying Ma, University of Melbourne, Melbourne, Australia, yima3@student.unimelb.edu.au; Cherie Sew, University of Melbourne, Melbourne, Australia, csew@student.unimelb.edu.au; Zhanna Sarsenbayeva, University of Sydney, Sydney, Australia, zhanna.sarsenbayeva@sydney.edu.au; Jarrod Knibbe, University of Queensland, St Lucia, Australia, j.knibbe@uq.edu.au; Jorge Goncalves, University of Melbourne, Melbourne, Australia, jorge.goncalves@unimelb.edu.au.

ACM 2573-0142/2024/9-ART282
https://doi.org/10.1145/3676529

research also indicates a strong correlation between users' decisions regarding the installation of a mobile app and their perceptions of the app, which are closely linked to their ability to control the app's access to information and its usage of that information [69].

However, managing privacy settings across a growing number of applications remains a complex challenge. For instance, users may need to navigate and click through multiple layers to modify certain settings - a convoluted process which can be seen as a barrier to accessibility. For example, Twitter's mobile app requires users to navigate five screen levels to toggle content personalization based on places users have been, a feature that is turned on by default regardless of the current location access setting on iOS. Furthermore, the use of different terminologies or privacy frameworks by various apps, and non-compliance of privacy labels on iOS [71] also leads to confusion and a decreased privacy management intention. This complexity is exacerbated by the fact that privacy policies are often long and inaccessible [55], hindering users' ability to effectively manage their privacy. Thus, as users install more apps, the task of maintaining privacy settings becomes more burdensome, leading to users experiencing privacy fatigue [15]. Moreover, the variation in users' privacy literacy [7] and awareness about privacy settings introduces another layer of complexity to this issue, affecting their ability to navigate and manage their privacy effectively.

Among all types of personal information, location data is notably important due to its potential to reveal latent details about an individual's habits, preferences, and lifestyle. For instance, a study conducted on Pokémon Go, the location-based mobile game, managed to collate users' movement patterns and daily routines while playing the game, which was then used to infer the game's effect on users' behaviour [4]. Revealing an individual's routines together with their location data can lead to cybercasing - the act of using location data to carry out real-world attacks like theft or robbery [27]. In addition, previous work presented scenarios where it was possible to find accurate addresses of anonymous Craigslist users, track a celebrity's location using Tweets, and determine a Youtube user's normal routine from their vacations [27]. This growing use of location-sharing features on social media platforms has empowered researchers to utilise geotagged data for a variety of studies, including human mobility, tourist flow analysis, and the observation of collective behaviours [32, 41, 42]. However, due to the sensitive nature of this information, if accessed by unauthorised parties or malicious users, it can lead to privacy violations, targeted advertising, and even more serious consequences, such as stalking or identity theft [13].

A study from 2012 examined how iPhone users manage their privacy settings, identifying different types of users [26]. However, their work did not analyse distinct categories or different levels of granularity in users' privacy control. A more recent study, while timely, based its quantification fully on self-reported settings data [20], lacking objective data on user behaviour. Other studies have investigated users' general privacy concerns across different apps [16, 63]. Although online privacy is a well studied topic, and previous literature have touched on location privacy from different angles, user perceptions and behaviours regarding location privacy benefits from continuous research in this area. This is particularly important given that smartphone operating systems, and the number of mobile apps as well as its use cases are constantly progressing. Therefore, it is pertinent to conduct in-depth research that focuses on location information privacy from the perspective of both user behaviour and location privacy expectations with recent location privacy control affordances. For instance, a significant update occurred with the release of iOS 14 in September 2022. This version introduced four distinct choices ("Always", "While Using the App", "Ask Next Time or When I share" and "Never") for app location settings, marking a pivotal change in user control over privacy [8], which we explored in our study. In addition, we also investigate the variations in location privacy settings among different app categories using naturalistic data, an aspect that has not been investigated in previous work.

In this study, we aim to explore how iPhone users' manage their location privacy settings on their smartphones within the context of different app types, with a particular focus on the factors that impact users' decisions, and the discrepancy between intention and behaviour. We then provide an in-depth investigation into users' location privacy concerns across different apps with varying degrees of location-based features.

Based on the research gaps identified above, in this work, we focus on two research questions:

- **RQ1**. What factors influence iOS users' intentions and actual behaviour in managing location privacy settings?
- **RQ2**. What are users' concerns and perceptions on location privacy between apps that leverage location information in different ways?

Our study advances the understanding of location privacy management on smartphones by contrasting users' privacy preserving intentions and actual behaviours. We highlight the role of privacy fatigue and usability perceptions in the decisions made by users regarding their location privacy. By examining users' location privacy concerns across various apps, we explore the significance of platform leadership and privacy-preserving features in shaping user trust and privacy perceptions, as well as the need for more uniform location privacy settings. Our findings provide crucial insights for informing the development of more intuitive and effective privacy controls on smartphones.

2 Related Work

In this section, We start by discussing users' general online location privacy behaviour and perceptions. We then examine location privacy perceptions in the context of different social media smartphone app types.

2.1 Online Location Privacy Behaviour and Perceptions

As users become more aware of the importance of safeguarding their personal information, there is an increasing concern that businesses or governments are not competent in handling this data. The Pew Research Center [24] reported in 2023 that approximately 71% of Americans were concerned with the online user data collected by the government, and 77% of Americans did not trust that social media platforms handles their personal data and privacy responsibly.

According to the Westin index [44], users can be categorised into three groups: privacy fundamentalists, those who are highly concerned with user privacy and favour strong public policy related to privacy rights; privacy pragmatists, those who value the choice of the user in deciding whether to share personal information; and privacy unconcerned, those who place little or no value on privacy rights and would willingly provide personal information. Similarly, Fisher et al. [26] found that iPhone users can be categorised as users who share location access to all apps, users who permit some apps access, and users who do not share location access with any apps. However, the study utilised screenshots provided by participants of their system's Location Services settings, meaning that the researchers did not have access to privacy settings within the apps. In another study, researchers found that users' personal motivation and privacy-related knowledge were crucial factors in their privacy preserving behaviour [20].

Interestingly, Furini and Tamanini [28] found that users who were initially unconcerned about privacy had a greater concern when they were exposed to the effortless process of obtaining personal and sensitive data through geotagged content on Twitter and Instagram as well as locating users in real time. Through analysing the quarantine app during COVID-19, researchers also gained insights into location-based apps, such as increasing transparency in the interface to alleviate stress, mental fatigue, and mistrust among users [70]. Furthermore, although everyday users are increasingly more aware of potential privacy threats [31, 72], some users still share location data [56] or other sensitive personal information when there are tangible benefits [30]. This discrepancy between user attitude and their actual behaviour is known as the “privacy paradox” – a phenomenon that has been both confirmed [49, 58, 66, 74] and debunked [17, 73] in previous studies. Additionally, the sharing of sensitive information could also stem from maladaptive responses of privacy resignation or helplessness due to the perceived belief that privacy infringement is inevitable [14, 67].

While users can control their privacy settings and modify location sharing permission for each app, Fawaz et al. [25] found that mobile apps are still able to profile users through embedded libraries that aggregate location data across different apps. Furthermore, Kollnig et al. [40] found a widespread issue of apps potentially violating data protection and privacy laws enacted by the US, UK, and EU. The same study also found that there is no discernible difference in which is better for user privacy between iOS or Android’s ecosystems. However, Apple’s iOS 14 and newer have updated privacy features, including the app developer’s self-reported privacy nutrition labels, and allowing users more granular control over app location data. Comparatively, Android 14 has similar granular control for apps’ approximate or precise location but lacks features like app tracking permissions. [2]

Thus, Apple’s latest privacy management tools provide us with an opportunity to investigate users’ current behaviours surrounding location privacy. Additionally, our study further investigates the “privacy paradox” by understanding how users perceive their online privacy through self-reporting, and comparing this to their actual location privacy behaviours.

2.2 Location Privacy Across Different App Types

The type of app and its features are important factors in users’ location privacy disclosure behaviours. Previous work has found that users mainly consider the perceived app value while having lower concern over privacy in their intention for installing hedonic apps but they contemplate over the perceived value of an utilitarian app and its privacy concerns [29]. Considering the growth in popularity of social networks and their location sharing capabilities, existing literature have contributed to the topic of location privacy by investigating user perception and behaviour on different social media apps. However, there is a lack of comparative research between distinct social media app types which have different location information sharing functionalities and capabilities.

Therefore, there is an opportunity to examine and compare user perceptions on different social media app types in the context of its location information sharing capabilities. Akdim et al. [1] found that most users consider Instagram as a hedonic app due to being used for entertainment [54] and its support of users’ psychological needs (e.g. the need to belong) through self-presentation [59]. Although Instagram is primarily an image-sharing platform, there are ways for users to share location information. For example, users can geotag their stories or posts, or disclose their location on their profile bio. Similarly, Twitter is not a Location-Based Social Network (LBSN) as its features and user relationships are not strictly dependent on location information. Users can geotag their posts similar to Instagram but with less precision as it can only find locations up to the neighborhood level. Yet the information users disclose on Twitter can still be used to infer their tweet locations, mentioned locations, and home locations [75] down to different granularities like city or geographic region [50]. However, unlike Instagram, most users perceive Twitter as a platform for procuring and sharing information instead as a fun, entertaining environment [48], to such an extent that it is categorised under ‘News’ on Apple’s App Store. On the other hand, an example of a popular LBSN is Yelp. Although the recommendation and review platform does not require members to display their real name, it is encouraged as they believe pseudonyms might

[2] Privacy control features for Android 14 (https://www.android.com/intl/en_au/safety/privacy/)

decrease the credibility of user contributions. Along with direct location sharing through reviews, check-ins, and geotags, these user-shared information can be further used to infer demographic attributes (age, gender, occupation) even if it was hidden by the users [46].

Table 1 presents some previous works that have compared at least two different social networking apps within the context of online privacy [12, 16, 29, 57, 62] and more specifically, location privacy [28]. However, these literature did not examine user perception and users' in-app location privacy behaviour in tandem. Thus, we aim to address the gap in the literature related to users' concerns and perceptions on location privacy by providing an in-depth investigation on these factors within Instagram, Twitter, and Yelp - three apps that utilise location information through various means.

Table 1. Existing literature that attempted to compare different social networking platforms in the context of online privacy or location privacy

Reference	Method of Analysis	Apps Analysed	App Type
Serafinelli and Cox [62]	Netnography, User Interviews	Instagram and Blipfoto	Both Photo Sharing
Choi and Sung [16]	Analytical, Survey	Instagram, Snapchat	Both Photo Sharing
Rashid and Zaaba [57]	App Evaluation	Facebook, Twitter, Instagram	Social Network, Microblog, Photo Sharing
Burkholder and Greenstadt [12]	App Evaluation	Amazon, Netflix, Yelp, OpenTable, TripAdvisor	Online Retailer, Reservation Service, Video Streaming Service, Recommender Systems
Furini and Tamanini [28]	Questionnaire, Behavioural Study	Twitter, Instagram	Microblog, Photo Sharing
Gu et al. [29]	Analytical, Imagery	Super Racing, Delicacy	Game, Information Service

3 Study Design

3.1 Procedure

We deployed an online survey-based experiment, with a specific focus on iPhone users. This choice was guided by the uniformity of the iOS operating system, which prevents vendors from distributing customised versions of the system. In addition, Apple has recently made several changes to their privacy policy which aims to provide users with more autonomy over individual app's privacy settings. There are two main tasks in our survey, which we describe next.

3.1.1 Task 1 (RQ1). The aim of this task was to explore the factors, shaping and influencing users' location disclosure intention and actual behaviour. In order to achieve this, we leveraged several validated measures that were used in previous studies, the details of which are provided in Appendix Table 7, Table 9 and Table 8. We summarise these measures below.

- **Usage Intention:** A dependent variable assessed using three items on a 7-point Likert scale, evaluating the extent of users' intentions to use location privacy settings on their smartphones [2, 47].
- **Actual Behaviour:** A dependent variable representing the ratio of apps that each participant denies location information access. Participants were requested to submit screenshots of their device's location privacy settings. These screenshots display the level of location access requested by each app installed by the user. This method has been employed in the previous work investigating location privacy behaviours of iOS users [26].
- **Privacy Fatigue (Burnout general survey):** A continuous variable assessed using six items on a 7-point Likert scale measuring the emotional exhaustion and cynicism users feel towards managing location privacy settings on smartphones [15, 61].

- **Internet Users' Information Privacy Concerns (IUIPC):** A continuous variable measured by ten 7-point Likert scale items, gauging user concerns about internet privacy, focusing on data control, awareness, and collection [39].
- **Usability:** A continuous variable measured by six 7-point Likert scale items. This construct relates to users' perceptions of the usefulness and ease of using location privacy settings on smartphones [21, 37, 68]. In this context, we utilize the concept of Technology Acceptance Model, which suggests that two specific beliefs, perceived usefulness, and perceived ease of use, are crucial in shaping a user's attitude toward utilizing a technology [3].
- **Online Privacy Literacy Scale (OPLIS):** A continuous variable measured by twelve single choice questions. This encompasses knowledge of institutional practices, technical data protection aspects, data protection laws, and strategies for data protection [52]. All EU-specific questions were omitted from this measure.

We also asked participants to rate their level of comfort with different app categories acquiring and using their location information, using a 7-point Likert scale (very uncomfortable to very comfortable). This data was used to further contrast usage intention with actual behaviour concerning location privacy settings across different app categories. Finally, we requested participants to elaborate on the reasoning behind their ratings.

3.1.2 Task 2 (RQ2). For Task 2, we aim to conduct a thorough investigation into user attitudes regarding the disclosure of their location information, location privacy concerns, and their perceptions and behaviours related to location-related in-app settings or features across three distinct applications – Twitter, Instagram, and Yelp.

Table 2. Differences between Instagram, Twitter, and Yelp

App Name	App Type	Main Features	Location-based Features
Twitter	Microblogging	View, post, and share Tweets	Tagging location to Tweets View content based on user's current location
Instagram	Photo and Video Sharing	Post media e.g. photos or 'reels'	Geotag in stories and posts
		Post 'stories' that are only viewable for 24 hours	Search for location
		View related and/or trending content	
Yelp	Crowd-sourced Recommender	Discover businesses	Search for businesses in current or specified locations
		Leave reviews for businesses	Check-in at businesses or places
		Upload photos relevant to the business	Receive push notifications about interesting nearby businesses and events
		Rate businesses & Participate in location-based forums	

App selection criteria: We selected the apps based on the following criteria. First, we selected apps that have social networking features that are *popular*, *familiar* and belong to different app categories. Twitter is ranked 2^{nd} in the News category, Instagram holds the 2^{nd} position in the Photo & Video category, and Yelp is ranked 17^{th} in the Food & Drink category. Second, the chosen apps have distinct location-based functionality and levels of in-app control. The 1^{st} ranked apps for each category were not chosen because Reddit (1^{st} in News) lacked location-based features, CapCut (1^{st} in Photo & Video) is a video editor, and Yelp is the top app within the Food & Drink category that heavily relies on its location-based features. Table 2 presents the differences as well as relevant features for these three apps. Both Instagram and Twitter allow you to tag locations in your posts. They utilise location to tailor the user's experience on the platform more effectively, and display advertisements for businesses and services that may be of interest to you. However, the level of precision varies between the two platforms. Twitter's location tagging is less precise, allowing tags only up to the neighbourhood level, while Instagram allows users to mark specific locations like buildings and restaurants. Yelp also uses location data to personalise the user experience, but in a different way, namely by sending push notifications about nearby places of interest. In addition, Yelp uses the location information to provide recommendations when the user is trying to find a place of interest.

Experimental flow: At the start of Task 2, we asked participants about their location privacy concerns for the three apps, with three choices of "Concerned", "Somewhat Concerned", or "Not Concerned". Participants were then asked to elaborate on their choices. This was followed by location-related questions regarding each of the apps, with the app presentation order being counterbalanced.

For Twitter we asked participants' about two specific features related to location services: "Personalise based on places you've been" and "Show content in your current location". First, we inquired if participants were aware that these two features were enabled by default on Twitter. Following this, we sought their preference regarding the default status of this feature, offering options to keep it on by default, turn it off by default, or do not care. Participants were also asked to provide the reasoning for their choices.

For Instagram, we explored user opinions regarding the location information guide page. This page explains three elements: how users can access the location service, how Instagram will use this information, and how users can control it. Initially, we asked participants to rate the necessity of displaying this guide page before they grant permission, using a 5-point Likert scale (not at all necessary to extremely necessary). Following this, we inquired whether they would recommend that other applications also present a similar location information guide before requesting user permission, offering options of "Yes", "No", or "Not sure". Additionally, we asked for open-ended feedback on their thoughts, suggestions, or concerns about the design and content of the location information guide page.

For Yelp, we focused on users' perceptions of the "Talk Location" feature, a location-based function that enables conversations with individuals in the users' current city. We inquired whether users had previously used this feature and posed an open-ended question about their motivations or reasons for using or not using this feature on Yelp, asking them to describe the factors that influenced their decision.

3.2 Recruitment & Data Processing

We recruited 76 participants from the U.S. (38 M, 38 F) through Prolific, specifically targeting iOS users. The survey collected the educational qualifications of participants, revealing a diverse range of backgrounds. The majority held Bachelor's degrees (31 participants, 40.79%), followed by some college but no degree (13 participants, 17.11%), Master's degrees (11 participants, 14.47%), Associate degrees (9 participants, 11.84%), and high school graduates (including GED) (8 participants, 10.53%). A smaller proportion possessed doctoral degrees (2 participants, 2.63%) or professional degrees such as JD or MD (2 participants, 2.63%). Additionally, the survey categorized phone usage patterns, with most participants spending 3-6 hours (32 participants, 42.11%) or 6-9 hours (18 participants, 23.68%) on their phones daily, while a smaller percentage reported using their phones for more than 9 hours (13 participants, 17.11%), 1-3 hours (11 participants, 14.47%), or less than 1 hour (2 participants, 2.63%). The details of participants' demographics can be found in the appendix (Table 10). We ensured that all participants frequently use the three apps specified in Task 2 via the filtering mechanism on Prolific. Participants were compensated using the payment scheme recommended by Prolific [22].

To improve data quality, for Task 1, we evaluated the quality of the photos uploaded and excluded participants who did not follow our instructions (N=12), such as those uploading incomplete or wrong images. Then, we employed Optical Character Recognition (OCR) technology to convert images from user-uploaded screenshots into text. Specifically, we used the pytesseract library [3], which is an implementation of Google's Tesseract-OCR Engine. Given that the accuracy of OCR technology can be influenced by factors such as image quality, font style, and layout complexity, we implemented a dual verification process to enhance data reliability. The OCR-generated data was independently checked by two researchers to confirm accuracy. Then we labelled all apps based on their iOS App Store category (e.g., *Navigation*, *Photo & Video*, *Social Networking*).

For Task 2, we excluded one participant for not providing any reasoning for their choices. We conducted a thematic analysis [18, 65] of the responses to the open-ended questions. We developed a coding framework aligned with our research objectives, guiding the coding and categorisation of our qualitative data. After several thorough reviews of the data, we gained a complete understanding and began the initial coding phase. During this phase, we segmented longer responses into smaller units whenever they covered multiple themes. Two researchers independently examined the transcripts, applying multiple rounds of coding to extract and summarise the themes. They then worked together to address any differences in their coding. When the predefined codes failed to sufficiently represent the data, we adjusted the coding framework—merging, splitting, modifying, or introducing new codes for more accurate data representation [45]. Additionally, all authors met frequently to review the data, discuss notes and discrepancies, and refine emerging themes until a consensus was reached. Ultimately, we organised the codes into a hierarchical structure of themes that we then used to present our findings.

4 Results

4.1 RQ1: Contrasting users' intentions and actual behaviour in managing location privacy settings

For Task 1, 64 participants provided valid submissions. The total number of app installations was 3,526, and among these, 587 were not granted location permissions. On average, participants had 55.1 (SD = 27.6) installed apps. The maximum number of apps recorded in our dataset for a single user was 160, and the minimum number was 8. Among these installed apps, there were 1,042 unique apps.

Coefficient	Estimate	Std. Error	Pr(>|t|)
(Intercept)	4.804	4.275	0.266
Age	-0.023	0.028	0.431
Gender[F]	0.532	0.679	0.437
Fatigue	-0.149	0.047	0.002**
Usability	0.151	0.060	0.014*
IUIPC	0.222	0.051	<0.001***
OPLIS	-0.303	0.195	0.126

Table 3. GLM Model for Usage Intention

Coefficient	Estimate	Std. Error	Pr(>|t|)
(Intercept)	0.176	0.244	0.474
Age	-0.001	0.002	0.413
Gender[F]	0.001	0.039	0.981
Fatigue	-0.000	0.003	0.882
Usability	-0.002	0.003	0.547
IUIPC	0.000	0.003	0.912
OPLIS	0.014	0.011	0.216

Table 4. GLM Model for Actual Behaviour

[3] https://pypi.org/project/pytesseract/

Below we present the outcomes of our analysis. We employed a Generalised Linear Model (GLM) to compare the effects of individual predictors to two dependent variables. The final model for the usage intention is shown in Table 3, with Conditional $R^2 = 0.49$.

Our analysis reveals that IUIPC had a significantly positive effect on the intention to use location privacy settings on smartphones ($\beta = 0.222,\ p < 0.001$, effect size = 0.43). This indicates that users who are more concerned about their online privacy are also more likely to use these settings. Conversely, an increase in privacy fatigue negatively affects this intention ($\beta = -0.149,\ p = 0.002$, effect size = -0.35), suggesting that the more fatigued the users feel about privacy, the less likely they are to engage with these settings. Furthermore, we also found that the users' perception of the usability of the location privacy settings system on their smartphones also positively influences their intention to use it ($\beta = 0.151,\ p = 0.014$, effect size = 0.27).

However, we did not find any factors that impacted the actual behaviour of the participants (Table 4).

4.1.1 Privacy Location Settings across Different App Categories. To further contrast participants usage intention and actual behaviour, we analysed how participants thought about and approached their location privacy settings for different app categories. We plotted the proportion of different levels of location permissions of apps in different categories (Figure 1). We excluded app categories that had fewer than 25 installations from our analysis (e.g., Books and Graphics & Design) due to inadequate sample size which proved challenging for meaningful analysis.

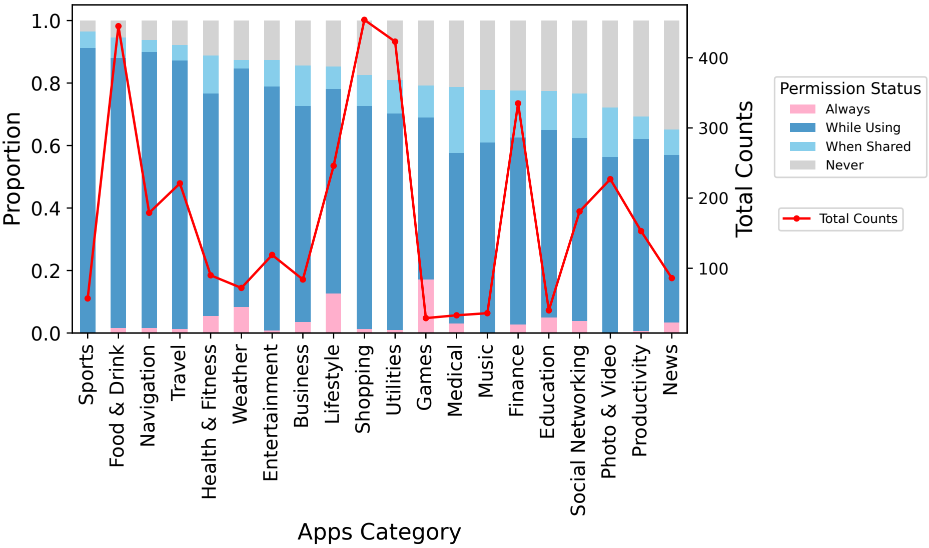

Fig. 1. Proportion of Different Levels of Location Information Access by App Category

Participants were the least concerned about their location privacy with regard to the *Sports* (e.g., ESPN, NFL) category, with 91.23% installations opting for access "While Using" the app and 5.26% allowing access only "When Shared". The *Food & Drink* (e.g., Yelp, McDonalds) category also had a remarkably high rate of participants granting location permissions, with 1.57% "Always", 86.52% "While Using" and 6.52% "When Shared". This is closely followed by the *Navigation* (e.g., Maps, GoogleMaps) and *Travel* (e.g., Uber, Lyft) categories, showing a similar trend with 88.27% and 85.97% respectively in the "While Using" option.

On the contrary, the *News* (e.g., Reddit, Twitter) category had 34.88% of participants denying location access, followed by the *Productivity* (e.g., Calendar, Reminders) category, where 30.72% of participants chose to "Never" share their location information. Interestingly, in the *Social Networking* (e.g., Facebook, Messenger) category, 23.20% of participants do not allow location access.

We found that participants' self-reported intentions were only partially aligned with their actual behaviour with regards to how they setup their location privacy settings for different app categories (Figure 2). For categories such as *Food & Drink*, *Shopping* (e.g., Walmart, Target) , and *Health & Fitness* (e.g., Sweatcoin, Strava) , participants demonstrated a high tolerance for allowing location access.

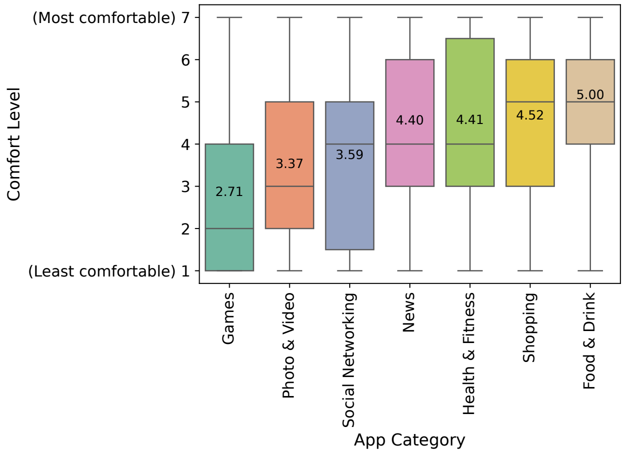

Fig. 2. Self-Reported Comfort Level of Sharing Location Information for Different App Categories

However, there is also a notable discrepancy between self-reported comfort levels and actual behaviour. A striking example of this is seen in the *Games* (e.g., Pokémon GO, Blockudoku) category. Despite being ranked as the least comfortable in terms of location data access by participants, *Games* exhibited a lower rate of access denial compared to categories such as *News* and *Social Networking* apps. Intriguingly, *Games* also had the highest rate of consistent location access ("Always") among all categories. Similarly, *News* apps, which participants reported as relatively comfortable in terms of location data access, had the highest rate of access denial in actual usage patterns.

In addition, we employed the Kruskal-Wallis test to determine whether there were statistically significant differences in the self-reported comfort level across various app categories. Given the non-parametric nature of the data, the Kruskal-Wallis test was chosen as it does not assume a normal distribution. The test revealed significant differences among the app categories ($H = 71.82$, $p < 0.001$). To further investigate which specific categories differed from each other, Dunn's test for multiple comparisons with Bonferroni correction was conducted as a post-hoc analysis. This analysis pinpointed significant discrepancies between several pairs of categories, the p-value result is shown in Table 5. For example, the Games and Photo & Video categories show significant statistical differences when compared with News, Health & Fitness, Shopping, and Food & Drink. For Social Networking Apps, there exists a significant difference compared to both Shopping and Food & Drink Apps.

4.1.2 Qualitative Findings. Several participants expressed willingness to share location data with apps that provide direct, tangible benefits. This is evident in statements like, *"For restaurant or*

Table 5. Post-Hoc Pairwise Comparisons Between Application Categories

	Photo & Video	**Social Networking**	**News**	**Health & Fitness**	**Shopping**	**Food & Drink**
Games	0.87	0.15	4.66×10^{-6}	3.75×10^{-6}	6.11×10^{-7}	4.82×10^{-11}
Photo & Video		1.00	0.04	0.03	0.0095	1.36×10^{-5}
Social Networking			0.27	0.24	0.09	3.23×10^{-4}
News				1.00	1.00	1.00
Health & Fitness					1.00	1.00
Shopping						1.00

drink recommendations, having your location on so it can recommend you places nearby is a useful feature" (P2), and *"My reasoning is mainly based on convenience and how frequently I use these apps and services"* (P33). Moreover, participants feel more comfortable sharing their location information with apps that have a clear and practical connection to their physical surroundings, as one participant stated: *"I'm more comfortable with apps that connect me to the physical world"* (P4). This includes apps for news, food and drink, and shopping, which use location data to provide localised content or services. These responses highlight the perceived value in location tracking when it enhances the app's functionality or user experience.

The perceived intent and trustworthiness of the app can also influence a person's willingness to share location data. Particularly with apps that do not have a clear need for location data, e.g., games and social networking, participants stated *"I feel a general dislike towards these types of companies having access to my information since it feels like they would use that information just to try to target me in the future. I have no interest in it so I would not feel the most comfortable giving them my information"* (P73). This highlights concerns over safety and the potential misuse of location data are prominent.

Furthermore, participants expressed discomfort with apps that default to sharing location data. This is evident in statements such as *"For example if I select a picture to share on an app or website from my phone, on the bottom it defaults to "location on" so I've been having to manually uncheck this option. I don't really like the default being to share, and would feel better if the default was not to share location for my photos/video"* (P11). This highlights a desire for a more privacy-conscious default setting and greater control over the decision to share personal data.

4.2 RQ2: Contrasting User Location Privacy Concerns Across Twitter, Instagram, and Yelp

For Task 2, we analysed a total of 75 valid responses. Initially, we examined the factors influencing users' concerns (or lack of concern) about their location privacy across these apps. Subsequently, we explored users' perceptions of privacy regarding specific location-related features within the apps.

4.2.1 Factors that cause Location Privacy Concerns. We found that for Twitter, 20% of participants were concerned, 22% somewhat concerned, and 58% not concerned about their location privacy, while for Instagram, 9% were concerned, 51% somewhat concerned, and 40% not concerned. Finally, regarding Yelp, 11% expressed concern, 36% were somewhat concerned, and 53% showed no concern regarding location privacy (Table 6).

Interestingly, users' attitudes towards Twitter were quite polarised, with the highest proportion of participants among the three apps expressing either high concern or no concern at all. Similarly, regarding participants' actual settings, shown in Figure 3, Twitter had the largest percentage selecting "Never" for location sharing. Conversely, Yelp users predominantly choose "While Using" as their preferred setting. Instagram presents a balanced spread across all three choices, indicating a more varied approach to location sharing among its users.

Table 6. Participants' Concerns Distribution across Location Privacy on Different Social Media Platforms

Concern Level	Twitter	Instagram	Yelp
Concerned	20%	9%	11%
Somewhat Concerned	22%	51%	36%
Not Concerned	58%	40%	53%

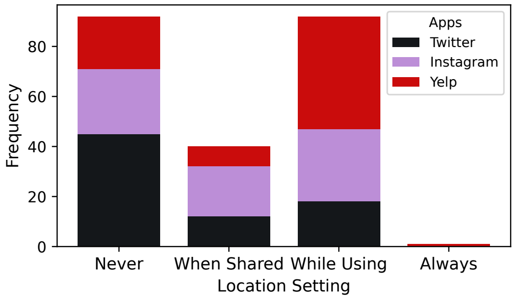

Fig. 3. System-Level Location Settings for the Three Chosen Apps

Regarding the reasons behind their choices, we conducted a qualitative analysis and categorised them into themes as depicted in Figure 4. In general, participants were concerned about their location privacy for the following reasons.

Misuse of Geolocation Data: These participants are concerned about the potential for their location information to be misused, including the potential advertisers spamming ads based on location and the possible sharing of their information with third parties without explicit consent. For instance, one participant expressed unease about the precision of targeted advertising, saying, *"It sometimes feels as if IG (Instagram) knows me too much. If I have a discussion with a friend about a product, the next ad I am seeing on IG (Instagram) is the product"* (P20 × Somewhat Concerned).

General Distrust of Online Information Privacy: This distrust is rooted in a combination of factors, including previous experiences of data breaches, the opaque nature of data usage policies of major tech companies, and the perceived inability or unwillingness of these entities to protect user data effectively. *"Instagram is owned by Meta. I feel like I've read over the years that Instagram is one of the worst offenders of collecting user information, so I am definitely somewhat concerned about location privacy on Instagram"* (P36 × Somewhat Concerned).

For Twitter and Instagram specifically, participants concerns revolved around the following issues.

Prevalence of Hacking and Identity Theft: Users are concerned about the risks tied to hacking and identity theft, a sentiment fuelled by their observations and experiences with these platforms. The apprehension is not unfounded, as instances of security breaches and unauthorised data access have been reported, for example, a participant stated *"It's been hacked before, so I'm a little concerned"* (P24 × Somewhat Concerned).

Platform Integrity and User Experience: Users worry about the proliferation of bots, fake accounts, misinformation, and a general degradation of the platform's community standards. For instance, one participant expressed *"Twitter is full of people that are hateful, bots (people paid to post propaganda,* *especially Russian propaganda, political propaganda in general, etc), has exploded. Separately, my username is a Russian language word, so that has made my account interesting to hackers, so I try to give little info there, I turn on settings only as needed for work"* (P55 × Concerned).

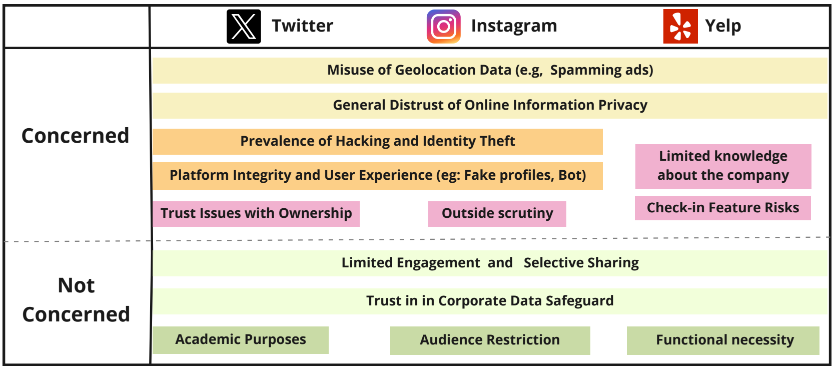
Twitter
Instagram
Yelp
Concerned
Misuse of Geolocation Data (e.g, Spamming ads)
General Distrust of Online Information Privacy
Prevalence of Hacking and Identity Theft
Platform Integrity and User Experience (eg: Fake profiles, Bot)
Limited knowledge about the company
Trust Issues with Ownership
Outside scrutiny
Check-in Feature Risks
Not Concerned
Limited Engagement and Selective Sharing
Trust in in Corporate Data Safeguard
Academic Purposes
Audience Restriction
Functional necessity

Fig. 4. Factors Influencing User Concerns or Indifference about Location Privacy of the Three Chosen Apps

Specific to Twitter, participants highlighted *Trust Issues with Ownership*, as a larger number of responses expressed a lack of trust in Elon Musk and the changes he may have brought to the platform. Concerns are not just about the potential misuse of personal information but also about the broader implications of his control over the platform. *"Twitter has been in shambles since Elon Musk took over and I'm concerned over the security of the app"* (P24 × Somewhat Concerned).

For Instagram, participants reflected on the impact of *Outside Scrutiny*, with fear over their accounts being accessed by familiar individuals, such as ex-partners, which amplifies their discomfort with the idea of being monitored. One participant candidly shared, *"I don't want my ex knowing what I'm doing"* (P34 × Somewhat Concerned). This concern underlines a profound desire for personal spaces and information to remain private, safeguarded from unwelcome scrutiny.

Finally, for Yelp, participants' specific concerns originate from two main sources.

Limited Knowledge about the Company: Participants indicated a lack of understanding of Yelp's handling of user data, contributing to their worries: *"I don't know much about the company but I imagine they aren't honest with their user data"* (P59 × Somewhat Concerned).

Check-in Features Risks: While Yelp's utility for finding restaurants and services is acknowledged, there's a nuanced apprehension about the visibility of one's location data through check-ins and reviews. Participants stated that they worry about the implications of such visibility, from the invasion of privacy to potential physical vulnerability. *"A lot of my check-ins and reviews on Yelp are local places so having that kind of information exposed online feels a bit unsafe and I am somewhat concerned"* (P21 × Somewhat Concerned).

4.2.2 Factors that cause Indifference with Location Sharing. On the contrary, some participants have a more relaxed stance towards privacy concerns on these social media platforms for the following reasons.

Limited Engagement and Selective Sharing: Many participants expressed a lack of concern for their privacy due to their selective sharing habits. Their interactions are characterised by a cautious approach to what they post, focusing on content that does not reveal sensitive details about their lives. This cautious engagement minimises perceived privacy risks, as they believe that they are not providing the platform with data that could be exploited. Supporting this perspective, a participant stated: *"I don't post a lot of private information"* (P13 × Not Concerned).

Trust in Corporate Data Safeguards: This set of participants feels confident in the privacy protections and security technology and algorithms implemented by large companies. For instance, a participant stated that *"I trust them and believe being such a big company they have the right technology to protect my info"* (P50 × Not Concerned).

Regarding Twitter specifically, some participants mentioned that their use of the platform for *Academic Purposes* limits exposure of personal information, naturally reducing privacy worries due to the professional or educational nature of their posts. *On Instagram,* participants mentioned that the option to set accounts to private was identified as a key method for reducing privacy concerns. This feature restricts access to user content, offering enhanced control over their online presence and proactively safeguarding their privacy by selectively curating their audience. Finally, for *Yelp*, participants raised the point of *Functional Necessity*, where the use of location services is deemed important for the app's perceived utility. Participants accept location sharing as integral to the experience, enabling them to receive personalised recommendations and discover local businesses. As one participant mentioned *"I am not worried about my location being shared as a general rule. Sharing is would likely be more beneficial as I can get better recommendations for places near me"* (P2 × Not Concerned).

4.2.3 Privacy Perceptions of Specific Location-Related Features.

Twitter: Default Location Feature Activation. Regarding the default activation of location-based features, the majority of participants were unaware that these settings are enabled from the outset (Personalise based on places you've been feature (Personalisation): 74.7% users were unaware; Show content in your current location feature (Show): 76.0% users were unaware). Regarding participant preferences for the default state of these features, only a small proportion expressed a preference for these features to be enabled by default (Personalisation: 6.7%; Show: 9.3%). They appreciate the personalised experience it offers and believe it enhances their use of the app and provides content that is relevant to their interests or location, which makes the platform more engaging and relevant.

However, the majority of users would prefer if these features were turned off by default (Personalisation: 70.7%; Show: 70.7%). From the qualitative analysis, we identify the reasons for this preference with the following themes.

User Autonomy and Informed Consent: Participants expressed a desire for autonomy in deciding whether to activate location-based features, emphasising the need for informed consent. For instance, one participant stated that *"I prefer having informed consent over my information being shared and personalising based on tracking me"* (P11).

Skepticism towards Location-based Personalisation: Some participants were concerned about it being invasive or unnecessary for the platform experience, favouring a more generic content experience that respects their privacy over targeted content based on their location. As stated by one participant: *"I don't want content based on my current location, it feels very invasive"* (P18).

Instagram: Location Information Guide/Policy Page. 81.8% of participants — combining those who deemed it (58.4% choose "Extremely Necessary" and 23.4% "Very Necessary") — think it is imperative to present this location information guide page before granting permission. In addition, a predominant 89.3% advocated for the implementation of a similar location information guide page across other applications before permission solicitation.

Our qualitative analysis reveals the underlying reasons for this strong preference with the following themes.

Appreciation for Transparency and Clarity: Participants appreciated the transparency and clarity of the information presented. For instance, one participant mentioned, *"I like that it shows why they use it and I like that it shows you how to control it"* (P36). Another stated, *"It's clear, open and honest. This should be a requirement for every app"* (P24). These comments underscore the value placed on straightforward and accessible information about location data usage and management.

Highlight and Detail the Potential Risks: A segment of the participants called for more detailed information to be provided, particularly regarding data use and privacy. As one participant put it, *"They still use IP address to get general location, I find that to be concerning. I think these things should be made clearer and more obvious"* (P18), indicating a desire for greater transparency about data collection practices. At the same time, participants also highlighted the need for more information especially on potential risks of disclosing location information, with statements like: *"I don't like that it never mentions the potential harms"* (P45).

Prioritise Privacy for Default Settings: The preference for more user control was clear, with suggestions for default settings that prioritise privacy. *"It should come as off, then show this to user"* (P65). This indicates a preference towards a proactive approach to user consent, emphasising the importance of giving users the initial choice about sharing their location data.

Educational Value: The guide's role in educating users was frequently mentioned, with participants recognising its value in making informed decisions. For instance, one participant stated that *"The Location Information Guide page is an asset for people and I think that this educates them on their location settings, which is really good"* (P60). This reflects the positive reception to the guide's educational content and presentation style.

More unified experience: Although most participants thought this feature is useful and effective, one participant raised that *"Doing this on an app-by-app basis leads to confusing & conflicting user experiences. Apple could expand their built-in iOS location prompts to include more information like this, as well as simplified "opt-out" or "forget my info" buttons and workflows"* (P6). This feedback underscores the importance of consistency and simplicity in user interactions. By uniforming or centralising the location privacy setting mechanisms, users can benefit from a unified experience that reduces complexity and enhances understanding.

Interactive privacy policy/guide consent: Enhancing the interactivity of privacy policy consent can improve user engagement and ensure that users are fully aware of the implications of their consent decisions. As mentioned by one participant: *"I think that they should make the information easier to see and make you scroll through something before confirming"* (P1).

Yelp: Talk Location. Out of 75 users, only 2 reported having used this function previously. The vast majority have never used it, citing the following reasons.

Use for Specific Purposes Only: Participants view Yelp totally as a tool for finding and reviewing restaurants, not as a social platform with statements like: *"I have no plans of using Yelp as a social media site. I just use it to look at food and review food from time to time. This feature is purely a social media feature and I have zero interest in it"* (P3). This indicates that the primary use case for Yelp among these users is to access local business information and reviews, rather than to engage in social interactions.

Unawareness of Feature Existence: In addition, a significant portion of the participants expressed that they were not aware of this feature. For example, one participant states that *"I have not used it because I was not aware of this feature"* (P49).

Privacy Concerns and Discomfort with Strangers: Many expressed unease at the thought of sharing personal information with unknown individuals. For example, one participant stated that *"I don't like sharing stuff about me with strangers in my area"* (P11).

5 Discussion

In this section, we discuss the privacy paradox between users' intentions and actual behaviours in managing location privacy on iOS devices. Furthermore, we reflect on users' privacy concerns across different types of apps. We synthesise key insights that can be leveraged to improve location privacy management on smartphones.

5.1 Location Privacy Management Intention and Behaviour

Our study underscores the significant impact of several factors on the usage intention of location privacy controls. For instance, the continuous exposure to privacy-related decisions and information overload (i.e., privacy fatigue [15]) can lead to disengagement, posing a challenge for designers and policymakers. At the same time, the influence of interface usability also highlights the need for designing user-friendly privacy interfaces that can encourage engagement, particularly among less tech-savvy users. Unsurprisingly, we also found a positive impact of IUIPC on usage intention, with participants with greater privacy concerns also stating their intention to actively manage their privacy settings.

However, the lack of significant factors impacting actual behaviour, as opposed to usage intention, denotes the presence of the "privacy paradox" phenomenon [66] among our participants, even with the recent updates and improvements to the iOS privacy management settings. This discrepancy could be attributed to various factors, such as the complexity of privacy settings, habitual usage patterns, or a general inertia in altering default settings. Further work is needed to better understand these factors and cater more precisely to individual user's needs.

Interestingly, our results also reveal a distinct dichotomy in users' location privacy concerns between hedonic and utilitarian apps. Previous research found that users place little weight on privacy concerns when deciding on hedonic apps [29]. However, our results show that users' self-reported data demonstrate a significant higher propensity to share location data with utilitarian apps (e.g., Food & Drink Apps, Shopping Apps and Health & Fitness Apps), perceived as offering tangible benefits and essential services. This willingness to share stems from the direct utility these apps provide, enhancing daily tasks and personal efficiency. Conversely, hedonic apps (e.g., Games Apps and Photo & Video Apps), which primarily serve entertainment and social networking purposes, see more resistance from users in granting location access. This indicates a more deliberate consideration and awareness by users, who prioritise the utility and perceived essential nature of utilitarian apps, thus demonstrating a greater willingness to share location data with them.

In addition, previous work has highlighted that mobile gaming apps are the most "data-hungry", collecting users' data through subtle pop-ups and checkboxes to provide it to third parties for advertising purposes [36]. Similarly, our study's findings also reveal that, compared to other app categories, the games category has the highest frequency of users selecting the "Always" option for actual location settings. This observation in gaming apps raises concerns about the challenge it poses to the goal of minimising sensitive data access and collection. Furthermore, this practice does not align with the broader principles of different privacy regulations and frameworks, something that both policymakers and users should consider.

5.2 Differences in Location Privacy Concerns Across Twitter, Instagram and Yelp

Interestingly, our findings show that there was a higher proportion of participants who had a high degree of concern (excluding those that were just somewhat concerned) about location privacy within Twitter when compared to the two other apps we explored. This heightened concern was attributed to Elon Musk's ownership of the platform, showing that the leader's public persona and actions can profoundly impact user trust. This has ramifications in terms of users' willingness to use location-based features due to their lack of trust in the platform [9, 10]. Simultaneously, Twitter exhibited the highest proportion of participants unconcerned about privacy among the three apps analysed. This opposing perspective can be linked to the platform's usage purposes. For instance, academic or professional use leads to more curated and carefully selected content, contributing to a perception of lower risk. This careful curation of profiles and content likely influenced participants' reduced concern over privacy on the platform.

Moreover, there was notable concern among participants regarding hacking, identity theft, fake profiles, and bots on Twitter and Instagram but not on Yelp. This discrepancy can be attributed to the distinct nature of the apps: Twitter and Instagram are primarily viewed as social platforms, while Yelp is more tailored towards providing recommendations and serving specific needs without the same level of social engagement found in the other two apps. This finding is inline with recent work showing a predominant distrust among users towards Facebook and other online social networks in their ability to safeguard the integrity of their platform, when compared to other types of apps [23]. Smartphone operation systems should consider allowing for system-wide privacy settings on particular apps types. This approach could potentially reduce users privacy fatigue [15] and enable a more simple but still targeted approach to privacy management on smartphones.

Furthermore, 60% of the participants are either concerned or somewhat concerned about their location privacy on Instagram. Our qualitative findings indicate that this is also partially due to concerns regarding outside scrutiny, such as that from ex-partners. Instagram allows users to restrict a post or reel to just close friends by selecting the audience option. However, there may be instances where a user wishes to post to a broader audience but is currently unable to prevent that certain individuals see the tagged location. Finally, participants highlighted significant privacy concerns with Yelp's check-in feature. Previous work has shown that there is an important trade-off between user experience and privacy, where features like check-ins, despite their appeal, pose privacy risks by potentially exposing personal information [38]. This trade-off highlights the need for further privacy preserving efforts to alleviate users' concerns, in order to achieve a balance between appealing features that contribute to community engagement and the protection of personal privacy.

5.3 Towards Better Location Privacy Management on Smartphones

The inconsistency in privacy settings across different apps presents a challenge for users attempting to manage their location privacy effectively. The distinct frameworks and terminologies employed by different platforms can lead to confusion, and a reduced intention of location data control and management. Consequently, there is a clear need for more uniform privacy settings across apps, as suggested in our qualitative findings. In view of this, one potential approach to achieving uniform privacy settings is through the use of privacy management tools or software. These tools are designed to centralise privacy controls [51], allowing users to set their preferences once and have them applied across different services.

Another aspect of uniform privacy settings involves the standardisation of privacy controls and options across different platforms. Previous research indicates that consistency in formatting and terminology helps consumers in becoming familiar with and comparing practices across privacy labels [19, 35]. Furthermore, although with multiple benefits, there are notable challenges associated with the current implementation of privacy labels, such as one one-time setting mechanism for developers, less motivation for users to take action and different requirements between iOS and Android [6]. Therefore, to support the effective privacy management experience across the platforms, there is a pressing need to use more common terminology and user interfaces to make it easier for individuals to understand and manage their privacy preferences. In addition, operating systems could offer educational content that explain the significance of privacy labels and how to use them effectively. Educating users about the implications of data privacy and the tools available to manage it has the potential to increase their willingness and ability to engage with privacy settings. From a regulatory perspective, the concept of uniform privacy settings may also relate to efforts to establish consistent privacy standards across different countries or industries.

Furthermore, several works have explored engaging users with privacy and security notices through interactive techniques [33, 34]. Our study further emphasises the need for more interactive privacy consent frameworks. These frameworks are designed to do more than just educate; they aim to provide users with comprehensive knowledge, enabling a user base that make informed decisions about their personal data. Also, in line with the result of Schaub et al. [60], our study shows the demand from users for highlighting potential risks in privacy consent rather than just benefits, to enhance users' privacy awareness. Although this approach may sometimes go against app developers priorities, it can help users manage their personal data effectively through a more transparent, user-centric consent process.

5.4 Limitations & Future Work

Our work has several limitations. First, our participant sample does not fully encompass the diversity of user perspectives regarding location privacy on smartphones. Our study focused on iOS users, which limits the generalisability of our findings to users of other operating systems, such as Android. The differences in user trust in different OS, user interface design, and privacy settings options between platforms can lead to varying user experiences and privacy concerns as well as management strategies. Future studies should aim to include a broader range of participants, extending beyond iOS users to incorporate those with different operating systems. This would enable a comparative analysis of privacy management practices across platforms, offering a more comprehensive view of mobile location privacy concerns. In addition, while we label each app based on its classification in the iOS App Store, it is important to acknowledge that certain apps may serve multiple purposes, and publishers have the discretion to select the category under which they list their apps. This introduces a potential limitation to our study's task1 Apps category-related analysis.

Second, for Task 2, we focused on three apps, namely Twitter, Instagram, and Yelp, chosen for their popularity and distinct location-based features. However, the vast ecosystem of smartphone applications encompasses a wider range of apps with unique privacy considerations. Consequently, some of our findings may not be directly applicable to other apps with different functionalities or privacy policies. Future research should consider a wider array of applications to provide a more comprehensive understanding of location privacy management. Finally, future work could employ mixed-methods approaches, such as combining surveys with in-depth interviews, observations, or log data analysis, which could provide a richer understanding of how users navigate in-app location privacy settings.

6 Conclusion

In this paper we provide an in-depth investigation of iOS users perspectives on location privacy management. Our findings indicate that privacy fatigue adversely affects users, while the perceived usability of the settings interface positively influences their intention to manage their location privacy. However, we also find a gap between users' intentions of location privacy management and their actual behaviours, highlighting the need for more simple and intuitive privacy controls. We also identify a dichotomy in location privacy concerns between hedonic and utilitarian apps, highlighting users' tendency to prioritise the utility and perceived essential services of utilitarian apps over the entertainment value of hedonic apps when it comes to preserving their location information.

In addition, we gathered participants' opinions on location-related settings across three distinct apps—Twitter, Instagram, and Yelp. Our findings revealed various reasons for users' concerns regarding their location privacy. Some of these reasons include but are not limited to trust issues with platform ownership, perceived company inability to maintain platform integrity, and outside scrutiny from other users. We highlight the importance of transparent, centralised, uniform, and standardised settings across apps to streamline privacy management and alleviate the burden on users. Overall, our work contributes to the broader effort of improving location privacy management on smartphones, aiming to increase user engagement with these controls.

References

[1] Khaoula Akdim, Luis V Casaló, and Carlos Flavián. 2022. The role of utilitarian and hedonic aspects in the continuance intention to use social mobile apps. *Journal of Retailing and Consumer Services* 66 (2022), 102888.

[2] Adi Alsyouf, Abdalwali Lutfi, Mohammad Al-Bsheish, Mu'taman Jarrar, Khalid Al-Mugheed, Mohammed Amin Almaiah, Fahad Nasser Alhazmi, Ra'ed Masa'deh, Rami J Anshasi, and Abdallah Ashour. 2022. Exposure detection applications acceptance: The case of COVID-19. *International Journal of Environmental Research and Public Health* 19, 12 (2022), 7307.

[3] Adi Alsyouf, Abdalwali Lutfi, Nizar Alsubahi, Fahad Nasser Alhazmi, Khalid Al-Mugheed, Rami J Anshasi, Nora Ibrahim Alharbi, and Moteb Albugami. 2023. The use of a Technology Acceptance Model (TAM) to predict patients' usage of a personal health record system: The role of security, privacy, and usability. *International journal of environmental research and public health* 20, 2 (2023), 1347.

[4] Ionut Andone, Konrad Blaszkiewicz, Matthias Böhmer, and Alexander Markowetz. 2017. Impact of location-based games on phone usage and movement: A case study on Pokémon GO. In *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services*. 1–8.

[5] Corey M Angst and Ritu Agarwal. 2009. Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS quarterly* (2009), 339–370.

[6] David G Balash, Mir Masood Ali, Xiaoyuan Wu, Chris Kanich, and Adam J Aviv. 2022. Longitudinal analysis of privacy labels in the apple app store. *arXiv preprint arXiv:2206.02658* (2022).

[7] Miriam Bartsch and Tobias Dienlin. 2016. Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior* 56 (2016), 147–154.

[8] Scott Bay and Jason Cohen. 2023. *How to Turn Off Location Services and Stop Your iPhone Apps From Tracking You.* https://au.pcmag.com/mobile-phones/57573/how-to-turn-off-location-services-and-stop-your-iphone-apps-from-tracking-you

[9] Laura F Bright, Hayoung Sally Lim, and Kelty Logan. 2021. "Should I Post or Ghost?": Examining how privacy concerns impact social media engagement in US consumers. *Psychology & Marketing* 38, 10 (2021), 1712–1722.

[10] Allison J Brown. 2020. "Should I stay or should I leave?": Exploring (dis) continued Facebook use after the Cambridge Analytica scandal. *Social media+ society* 6, 1 (2020), 2056305120913884.

[11] buildfire. 2024. *Mobile App Download Statistics & Usage Statistics.* https://buildfire.com/app-statistics/#:~:text=Research%20shows%20that%20there%20are,and%2030%20apps%20per%20month.

[12] Matthew Burkholder and Rachel Greenstadt. 2012. Privacy in online review sites. In *2012 IEEE Symposium on Security and Privacy Workshops*. IEEE, 45–52.

[13] Jeng-Chung Chen and Quang-An Ha. 2019. Factors affecting the continuance to share location on social networking sites: The influence of privacy concern, trust, benefit and the moderating role of positive feedback and perceived promotion innovativeness. *Contemporary Management Research* 15, 2 (2019), 89–121.

[14] Hichang Cho. 2023. Heterogeneous User Responses to Privacy Risks in Mobile Apps: Understanding the Dualistic Role of Privacy Risk Perceptions. In *Proceedings of the 25th International Conference on Mobile Human-Computer Interaction*. 1–7.

[15] Hanbyul Choi, Jonghwa Park, and Yoonhyuk Jung. 2018. The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior* 81 (2018), 42–51.

[16] Tae Rang Choi and Yongjun Sung. 2018. Instagram versus Snapchat: Self-expression and privacy concern on social media. *Telematics and informatics* 35, 8 (2018), 2289–2298.

[17] Emily Christofides, Amy Muise, and Serge Desmarais. 2009. Information disclosure and control on Facebook: are they two sides of the same coin or two different processes? *Cyberpsychology & behavior* 12, 3 (2009), 341–345.

[18] Victoria Clarke and Virginia Braun. 2017. Thematic analysis. *The journal of positive psychology* 12, 3 (2017), 297–298.

[19] Lorrie Faith Cranor. 2012. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.* 10 (2012), 273.

[20] Robert E Crossler and France Bélanger. 2019. Why would I use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap. *Information Systems Research* 30, 3 (2019), 995–1006.

[21] Ricardo de Sena Abrahão, Stella Naomi Moriguchi, and Darly Fernando Andrade. 2016. Intention of adoption of mobile payment: An analysis in the light of the Unified Theory of Acceptance and Use of Technology (UTAUT). *RAI Revista de administracao e Inovacao* 13, 3 (2016), 221–230.

[22] George Denison. 2023. *How much should you pay research participants?* Prolific. Retrieved May 14, 2023 from https://www.prolific.co/blog/how-much-should-you-pay-research-participants

[23] Sami Fathi. 2021. *More Users Trust Amazon and Google to Handle Their Personal User Data Than Apple, Survey Suggests.* https://www.macrumors.com/2021/12/22/survey-amazon-and-google-user-data-more-than-apple/

[24] Michelle Faverio. [n. d.]. Key findings about Americans and data privacy. https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/

[25] Kassem Fawaz, Huan Feng, and Kang G Shin. 2015. Anatomization and protection of mobile {Apps'} location privacy threats. In *24th USENIX Security Symposium (USENIX Security 15)*. 753–768.

[26] Drew Fisher, Leah Dorner, and David Wagner. 2012. Short paper: location privacy: user behavior in the field. In *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*. 51–56.

[27] Gerald Friedland, Robin Sommer, et al. 2010. Cybercasing the Joint: On the Privacy Implications of {Geo-Tagging}. In *5th USENIX workshop on Hot Topics in Security (HotSec 10)*.

[28] Marco Furini and Valentina Tamanini. 2015. Location privacy and public metadata in social media platforms: attitudes, behaviors and opinions. *Multimedia Tools and Applications* 74 (2015), 9795–9825.

[29] Jie Gu, Jing Tian, and Yunjie Calvin Xu. 2022. Private or not? The categorical differences in mobile users' privacy decision-making. *Electronic Commerce Research and Applications* 52 (2022), 101122.

[30] Eszter Hargittai and Alice Marwick. 2016. "What can I really do?" Explaining the privacy paradox with online apathy. *International journal of communication* 10 (2016), 21.

[31] Mariea Grubbs Hoy and George Milne. 2010. Gender differences in privacy-related measures for young adult Facebook users. *Journal of interactive advertising* 10, 2 (2010), 28–45.

[32] Julie Jiang, Jesse Thomason, Francesco Barbieri, and Emilio Ferrara. 2023. Geolocated Social Media Posts are Happier: Understanding the Characteristics of Check-in Posts on Twitter. In *Proceedings of the 15th ACM Web Science Conference 2023*. 136–146.

[33] Farzaneh Karegar, Nina Gerber, Melanie Volkamer, and Simone Fischer-Hübner. 2018. Helping john to make informed decisions on using social login. In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*. 1165–1174.

[34] Farzaneh Karegar, Daniel Lindegren, John Sören Pettersson, and Simone Fischer-Hübner. 2018. User evaluations of an app interface for cloud-based identity management. In *Advances in Information Systems Development: Methods, Tools and Management*. Springer, 205–223.

[35] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing privacy notices: an online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*. 1573–1582.

[36] Dhananjay Khatri. 2023. *Study reveals 38 out of 50 most popular mobile games are data-hungry apps.* https://www.cnbctv18.com/technology/study-reveals-38-out-of-50-most-popular-mobile-games-are-data-hungry-apps-16811261.htm

[37] Boonchai Kijsanayotin, Supasit Pannarunothai, and Stuart M Speedie. 2009. Factors influencing health information technology adoption in Thailand's community health centers: Applying the UTAUT model. *International journal of medical informatics* 78, 6 (2009), 404–416.

[38] Hyang-Sook Kim. 2016. What drives you to check in on Facebook? Motivations, privacy concerns, and mobile phone involvement for location-based information sharing. *Computers in Human Behavior* 54 (2016), 397–406.

[39] Sung S Kim and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Casual Model. *Information Systems Research* 15, 4 (2004), 336–355.

[40] Konrad Kollnig, Anastasia Shuba, Reuben Binns, Max Van Kleek, and Nigel Shadbolt. 2021. Are iphones really better for privacy? comparative study of ios and android apps. *arXiv preprint arXiv:2109.13722* (2021).

[41] Vassilis Kostakos, Denzil Ferreira, Jorge Goncalves, and Simo Hosio. 2016. Modelling smartphone usage: a markov state transition model. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Heidelberg, Germany) *(UbiComp '16)*. Association for Computing Machinery, New York, NY, USA, 486–497.

[42] Zoltán Kovács, György Vida, Ábel Elekes, and Tamás Kovalcsik. 2021. Combining social media and mobile positioning data in the analysis of tourist flows: A case study from Szeged, Hungary. *Sustainability* 13, 5 (2021), 2926.

[43] Oksana Kulyk, Paul Gerber, Michael El Hanafi, Benjamin Reinheimer, Karen Renaud, and Melanie Volkamer. 2016. Encouraging privacy-aware smartphone app installation: Finding out what the technically-adept do. (2016).

[44] Ponnurangam Kumaraguru and Lorrie Faith Cranor. 2005. Privacy indexes: a survey of Westin's studies. (2005).

[45] Yoonjoo Lee, John Joon Young Chung, Jean Y Song, Minsuk Chang, and Juho Kim. 2021. Personalizing ambience and illusionary presence: How people use "study with me" videos to create effective studying environments. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–13.

[46] Huaxin Li, Haojin Zhu, Suguo Du, Xiaohui Liang, and Xuemin Shen. 2016. Privacy leakage of location sharing in mobile social networks: Attacks and defense. *IEEE Transactions on Dependable and Secure Computing* 15, 4 (2016), 646–660.

[47] Chung-Feng Liu, Yung-Chieh Tsai, and Fong-Lin Jang. 2013. Patients' acceptance towards a web-based personal health record system: an empirical study in Taiwan. *International journal of environmental research and public health* 10, 10 (2013), 5191–5208.

[48] Ivy LB Liu, Christy MK Cheung, and Matthew KO Lee. 2010. Understanding Twitter usage: What drive people continue to tweet. (2010).

[49] Ying Ma, Qiushi Zhou, Benjamin Tag, Zhanna Sarsenbayeva, Jarrod Knibbe, and Jorge Goncalves. 2023. "Hello, Fellow Villager!": Perceptions and Impact of Displaying Users' Locations on Weibo. In *IFIP Conference on Human-Computer Interaction*. Springer, 511–532.

[50] Jalal Mahmud, Jeffrey Nichols, and Clemens Drews. 2014. Home location identification of twitter users. *arXiv preprint arXiv:1403.2345* (2014).

[51] Karola Marky, Verena Zimmermann, Alina Stöver, Philipp Hoffmann, Kai Kunze, and Max Mühlhäuser. 2020. All in one! user perceptions on centralized iot privacy settings. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–8.

[52] Philipp K Masur, Doris Teutsch, and Sabine Trepte. 2017. Development and Validation of the Online Privacy Literacy Scale (OPLIS). *Diagnostica* 63, 4 (2017), 256–268.

[53] Trevor T Moores. 2012. Towards an integrated model of IT acceptance in healthcare. *Decision Support Systems* 53, 3 (2012), 507–516.

[54] Bahri-Ammari Nedra, Walid Hadhri, and Mariem Mezrani. 2019. Determinants of customers' intentions to use hedonic networks: The case of Instagram. *Journal of Retailing and Consumer Services* 46 (2019), 21–32.

[55] Jonathan A Obar and Anne Oeldorf-Hirsch. 2020. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society* 23, 1 (2020), 128–147.

[56] Sameer Patil, Greg Norcie, Apu Kapadia, and Adam J Lee. 2012. Reasons, rewards, regrets: privacy considerations in location sharing as an interactive practice. In *proceedings of the Eighth Symposium on Usable Privacy and Security*. 1–15.

[57] Amira Farah Abdul Rashid and Zarul Fitri Zaaba. 2020. Facebook, Twitter, and Instagram: The Privacy Challenges. In *2020 International Conference on Promising Electronic Technologies (ICPET)*. IEEE, 122–127.

[58] Bernardo Reynolds, Jayant Venkatanathan, Jorge Gonçalves, and Vassilis Kostakos. 2011. Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours. In *Human-Computer Interaction – INTERACT 2011*, Pedro Campos, Nicholas Graham, Joaquim Jorge, Nuno Nunes, Philippe Palanque, and Marco Winckler (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 204–215.

[59] Siwi Sarita and Julia Suleeman. 2017. The relationship between the need to belong and Instagram self-presentation among adolescents. In *Universitas Indonesia Psychology Symposium for Undergraduate Research*.

[60] Florian Schaub, Rebecca Balebako, and Lorrie Faith Cranor. 2017. Designing effective privacy notices and controls. *IEEE Internet Computing* 21, 3 (2017), 70–77.

[61] Wilmar B Schaufeli. 1996. Maslach burnout inventory-general survey (MBI-GS). *Maslach burnout inventory manual* (1996).

[62] Elisa Serafinelli and Andrew Cox. 2019. 'Privacy does not interest me'. A comparative analysis of photo sharing on Instagram and Blipfoto. *Visual Studies* 34, 1 (2019), 67–78.

[63] Christina Shane-Simpson, Adriana Manago, Naomi Gaggi, and Kristen Gillespie-Lynch. 2018. Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital. *Computers in human behavior* 86 (2018), 276–288.

[64] statista. 2019. *Number of apps installed by mobile users in the United States as of 3rd quarter 2019.* https://www.statista.com/statistics/267309/number-of-apps-on-mobile-phones/

[65] Gareth Terry, Nikki Hayfield, Victoria Clarke, and Virginia Braun. 2017. Thematic analysis. *The SAGE handbook of qualitative research in psychology* 2 (2017), 17–37.

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

[67] Jayant Venkatanathan, Vassilis Kostakos, Evangelos Karapanos, and Jorge Gonçalves. 2013. Online Disclosure of Personally Identifiable Information with Strangers: Effects of Public and Private Sharing. *Interacting with Computers* 26, 6 (11 2013), 614–626. https://doi.org/10.1093/iwc/iwt058

[68] Viswanath Venkatesh, Michael G Morris, Gordon B Davis, and Fred D Davis. 2003. User acceptance of information technology: Toward a unified view. *MIS quarterly* (2003), 425–478.

[69] Na Wang, Bo Zhang, Bin Liu, and Hongxia Jin. 2015. Investigating effects of control and ads awareness on android users' privacy behaviors and perceptions. In *Proceedings of the 17th international conference on human-computer interaction with mobile devices and services*. 373–382.

[70] Paweł W Woźniak, Thomas Kosch, Eleonora Mencarini, Andrzej Romanowski, and Jasmin Niess. 2021. 'I would have Preferred an Ankle Tag': The Lived Experience of a Nationwide Quarantine App. In *Proceedings of the 23rd International Conference on Mobile Human-Computer Interaction*. 1–13.

[71] Yue Xiao, Zhengyi Li, Yue Qin, Xiaolong Bai, Jiale Guan, Xiaojing Liao, and Luyi Xing. 2023. Lalaine: Measuring and Characterizing Non-Compliance of Apple Privacy Labels. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 1091–1108. https://www.usenix.org/conference/usenixsecurity23/presentation/xiao-yue

[72] Mike Z Yao. 2011. Self-protection of online privacy: A behavioral approach. In *Privacy online: Perspectives on privacy and self-disclosure in the social web*. Springer, 111–125.

[73] Alyson Leigh Young and Anabel Quan-Haase. 2013. Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society* 16, 4 (2013), 479–500.

[74] Aristea M Zafeiropoulou, David E Millard, Craig Webber, and Kieron O'Hara. 2013. Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions?. In *Proceedings of the 5th Annual ACM Web Science Conference*. 463–472.

[75] Xin Zheng, Jialong Han, and Aixin Sun. 2018. A survey of location prediction on twitter. *IEEE Transactions on Knowledge and Data Engineering* 30, 9 (2018), 1652–1671.

A Appendix

Table 7. Question items for the Usage Intention, Privacy Fatigue and Usability measures

Measures	Items	References
Usage Intention	1. I intend to continue using the location privacy settings in the smartphone system to manage my privacy in the future.	[2, 47]
	2. My willingness to utilize the location privacy settings in the smartphone system is high.	
	3. I plan to continue using the location privacy settings in the smartphone system in the future.	
Privacy Fatigue	*Emotional Exhaustion*	[15, 61]
	1. I feel emotionally drained from managing with location privacy settings on my smartphone.	
	2. I am tired of online location privacy issues.	
	3. It is tiresome for me to care about online location privacy.	
	Cynicism	
	4. I have become less interested in online location privacy issues.	
	5. I have become less enthusiastic in protecting personal location information provided to online vendors.	
	6. I doubt the significance of online location privacy issues more often.	
Usability	*Perceived Usefulness*	[21, 37, 68]
	1. Using the location privacy settings in the iOS system improves the control I have over my personal data.	
	2. Using the location privacy settings in the iOS system makes managing my privacy less complex.	
	3. Using the location privacy settings in the iOS system effectively addresses my concerns about location privacy.	
	Perceived ease of use	[5, 53]
	4. Finding the location privacy settings from the smartphone system's homepage is easy for me.	
	5. I can easily get the location privacy settings in the smartphone system to reflect my preferences.	
	6. The structure and contents of the smartphone location privacy settings are easy to understand.	

Table 8. Question items for the modified IUIPC measure [39]

Constructs	Items	Question
Control (ctrl)	ctrl1	User online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
	ctrl2	User control of personal information lies at the heart of user privacy.
	ctrl3	I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
Awareness (awa)	awa1	Companies seeking information online should disclose the way the data are collected, processed, and used.
	awa2	A good user online privacy policy should have a clear and conspicuous disclosure.
	awa3	It is very important to me that I am aware and knowledgeable about how my personal information will be used.
Collection (coll)	coll1	It usually bothers me when online companies ask me for personal information.
	coll2	When online companies ask me for personal information, I sometimes think twice before providing it.
	coll3	It bothers me to give personal information to so many online companies.
	coll4	I'm concerned that online companies are collecting too much personal information about me.

Table 9. Question items for the OPLIS measure [52]

Questions	Answer Choices (Correct answer in bold)
1. Social network sites also collect and process information about non-users of the social network site.	**True** False Don't know
2. User data that are collected by social network site operators (e.g. Facebook) are deleted after five years.	True **False** Don't know
3. Companies combine users' data traces collected from different websites to create user profiles	**True** False Don't know
4. E-mails are commonly passed over several computers before they reach the actual receiver.	**True** False Don't know
5. What does the term "browsing history" stand for?	**...the URLs of visited websites are stored.** ...cookies from visited websites are stored. ...potentially infected websites are stored separately. ...different information about the user are stored, depending on the browser type.
6. What is a "cookie"?	**A text file that enables websites to recognize a user when revisiting.** A program to disable data collection from online operators. A computer virus that can be transferred after connecting to a website. A browser plugin that ensures safe online surfing.
7. What does the term "cache" mean?	**A buffer memory that accelerates surfing on the Internet.** A program that specifically collects information about an Internet user and passes them on to third parties. A program, that copies data on an external hard drive to protect against data theft. A browser plugin that encrypts data transfer when surfing online.
8. What is a "firewall"?	**A fallback system that will protect the computer from unwanted web attacks.** An outdated protection program against computer viruses. A browser plugin that ensures safe online surfing. A new technical development that prevents data loss in case of a short circuit.
9. Surfing in the private browsing mode can prevent the reconstruction of your surfing behavior, because no browser information is stored.	**True** False Don't know
10. Using false names or pseudonyms can make it difficult to identify someone on the Internet.	**True** False Don't know
11. Even though It-experts can crack difficult passwords, it is more sensible to use a combination of letters, numbers and signs as passwords than words, names or simple combinations of numbers.	**True** False Don't know
12. In order to prevent the access to personal data, one should use various passwords and user names for different online applications and change them frequently.	**True** False Don't know

Table 10. Participant Data

ID	Age	Gender	Education	Phone Usage Per Day
P1	23	F	Some college but no degree	3 - 6 hours
P2	21	F	Some college but no degree	More than 9 hours
P3	50	M	Bachelor's degree	3 - 6 hours
P4	29	M	Master's degree	1 - 3 hours
P5	20	M	Some college but no degree	6 - 9 hours
P6	45	M	Master's degree	1 - 3 hours
P7	26	F	Bachelor's degree	3 - 6 hours
P8	23	F	Associate degree in college	More than 9 hours
P9	28	M	Bachelor's degree	3 - 6 hours
P10	23	M	Bachelor's degree	1 - 3 hours
P11	43	F	Some college but no degree	More than 9 hours
P12	26	F	Some college but no degree	3 - 6 hours
P13	27	F	High school graduate	3 - 6 hours
P14	26	M	Bachelor's degree	6 - 9 hours
P15	41	M	Bachelor's degree	3 - 6 hours
P16	28	M	Associate degree in college	1 - 3 hours
P17	27	M	Bachelor's degree	3 - 6 hours
P18	48	F	Some college but no degree	More than 9 hours
P19	30	F	Bachelor's degree	6 - 9 hours
P20	31	F	Master's degree	3 - 6 hours
P21	26	M	Bachelor's degree	6 - 9 hours
P22	36	F	Associate degree in college	1 - 3 hours
P23	40	M	High school graduate	3 - 6 hours
P24	37	M	Associate degree in college	3 - 6 hours
P25	40	F	Doctoral degree	3 - 6 hours
P26	47	M	Bachelor's degree	3 - 6 hours
P27	34	F	Master's degree	3 - 6 hours
P28	24	F	Some college but no degree	1 - 3 hours
P29	35	M	Bachelor's degree	6 - 9 hours
P30	32	M	Bachelor's degree	1 - 3 hours
P31	64	F	Master's degree	3 - 6 hours
P32	33	F	High school graduate	6 - 9 hours
P33	25	F	Bachelor's degree	More than 9 hours
P34	30	F	High school graduate	3 - 6 hours
P35	49	M	Bachelor's degree	3 - 6 hours
P36	41	M	Bachelor's degree	6 - 9 hours
P37	28	M	Professional degree (JD, MD)	1 - 3 hours
P38	19	M	Some college but no degree	3 - 6 hours
P39	29	M	Bachelor's degree	1 - 3 hours
P40	51	F	Bachelor's degree	1 - 3 hours
P41	42	M	Bachelor's degree	3 - 6 hours
P42	36	F	Associate degree in college	More than 9 hours
P43	35	F	Professional degree (JD, MD)	More than 9 hours
P44	34	M	Associate degree in college	6 - 9 hours
P45	42	M	Bachelor's degree	3 - 6 hours
P46	60	F	Master's degree	Less than 1 hour
P47	28	F	High school graduate	6 - 9 hours
P48	37	F	Master's degree	3 - 6 hours
P49	24	M	Some college but no degree	More than 9 hours
P50	38	M	Master's degree	3 - 6 hours
P51	43	M	Master's degree	3 - 6 hours
P52	31	F	Bachelor's degree	3 - 6 hours
P53	34	M	Master's degree	3 - 6 hours
P54	23	F	Bachelor's degree	6 - 9 hours
P55	55	F	Bachelor's degree	Less than 1 hour
P56	51	F	Master's degree	More than 9 hours
P57	33	M	Bachelor's degree	More than 9 hours
P58	49	F	Bachelor's degree	6 - 9 hours
P59	27	M	Some college but no degree	3 - 6 hours
P60	39	M	Bachelor's degree	3 - 6 hours
P61	18	F	Some college but no degree	6 - 9 hours
P62	31	F	Associate degree in college	6 - 9 hours
P63	25	F	Bachelor's degree	3 - 6 hours
P64	22	M	High school graduate	3 - 6 hours
P65	35	M	Doctoral degree	3 - 6 hours
P66	20	F	Some college but no degree	6 - 9 hours
P67	34	F	Bachelor's degree	6 - 9 hours
P68	22	M	High school graduate	6 - 9 hours
P69	29	M	Some college but no degree	3 - 6 hours
P70	86	M	Bachelor's degree	More than 9 hours
P71	24	F	Bachelor's degree	More than 9 hours
P72	27	M	Associate degree in college	6 - 9 hours
P73	23	F	Bachelor's degree	6 - 9 hours
P74	39	M	Bachelor's degree	More than 9 hours
P75	43	M	High school graduate	1 - 3 hours
P76	31	M	Associate degree in college	3 - 6 hours

Received February 2024; revised May 2024; accepted June 2024