From Options to Action: Evaluating Adoption of Privacy Features in Fitness - Tracking Platforms

Pantelina Ioannou
Univeristy of Cyprus
Nicosia, Cyprus
ioannou.pantelina@ucy.ac.cy

Angeliki Aktypi
University of Cyprus
Nicosia, Cyprus
aktypi.angeliki@ucy.ac.cy

Elias Athanasopoulos
University of Cyprus
Nicosia, Cyprus
athanasopoulos.elias@ucy.ac.cy

Abstract

Fitness-tracking platforms, such as Strava and Garmin Connect, are increasingly popular and are reshaping how people monitor and share their physical activity. Given the sensitive nature of the data users share, these platforms implement a series of privacy features, including controls for profile visibility, activity sharing, and the specification of sensitive locations. In this paper, we present the first large-scale study aiming to quantify user adoption of privacy features on fitness-tracking platforms and to shed light on the reasoning behind identified trends. We apply a mixed-method. First, we provide a systematic categorization of the privacy features implemented across major fitness-tracking platforms. We then quantify their adoption, using the Strava and Garmin Connect platforms as our case studies, by analyzing 197,873 public activity records, revealing a gap between available controls and actual adoption. We complement our empirical evaluation by surveying 182 participants, confirming low adoption and identifying barriers. Our findings highlight limited use of privacy features and provide insights into the reasons for this trend, including a lack of awareness, perceived low necessity, concerns about functionality, and difficulties adjusting settings. We also discuss potential strategies to overcome these challenges.

CCS Concepts

• **Security and privacy → Human and societal aspects of security and privacy**.

Keywords

Fitness Tracking Platforms, Privacy Feature Adoption, User Behavior, Qualitative Study, Empirical Study

ACM Reference Format:
Pantelina Ioannou, Angeliki Aktypi, and Elias Athanasopoulos. 2026. From Options to Action: Evaluating Adoption of Privacy Features in Fitness - Tracking Platforms. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 21 pages. https://doi.org/10.1145/3772318.3791408

1 Introduction

The rise of fitness-tracking platforms has transformed how individuals monitor and share their physical activity. Platforms such as Strava [69] and Garmin Connect [13], offer users powerful tools to track workouts, analyze performance, and engage with an active online community. As of mid 2025, Strava counts more than 150 million users in over 185 countries [58, 67]. While these platforms provide significant benefits, they also introduce substantial privacy risks, as they collect and share sensitive user data, including location history, heart rate, and sleep patterns. In the literature, a significant amount of studies have documented vulnerabilities in fitness-tracking platforms [17, 33, 34, 50, 51, 86, 87], showing that publicly shared activity data can be exploited to infer sensitive information such as home addresses and daily routines.

To mitigate these risks, fitness networks have implemented a variety of privacy features, such as profile visibility controls, activity-sharing settings, and sensitive locations specification (e.g., home, work). However, despite the available privacy features and the growing awareness of digital privacy risks, users often fail to utilize the privacy features available to them. Prior research has examined users' awareness of privacy risks [81], understanding of threats [88], and information-sharing behaviors [63, 80]. To date, however, no empirical research has examined whether users actually enable the privacy settings designed to protect them, leaving the real-world adoption of these features by users undefined. Understanding this gap between feature availability and actual adoption is essential for designing more effective privacy mechanisms.

In this paper, we present the first systematic, mixed-methods evaluation of privacy feature adoption on fitness-tracking platforms. We combine (i) a large-scale empirical analysis of 197,873 publicly available user records from Strava and Garmin Connect, and (ii) a user study with 182 participants to understand self-reported adoption and the reasons for non-use. Our approach captures both measurable user behaviors and reported perspectives, offering a comprehensive picture of privacy feature engagement. By combining empirical measurements with survey insights, we provide both quantitative adoption rates and qualitative explanations of why adoption remains limited. To uphold ethical standards, we received approval from our National Ethics Board for both the analysis of publicly available data and the conduct of the user study.

Our findings indicate that users of fitness-tracking platforms largely neglect available privacy protections, leaving personal fitness data exposed. Only 36.42% of users set their profiles to private, while the majority (63.58%) keep them fully public. Activity-level controls are even less utilized, with only 2.12% of Strava activities applying additional restrictions and just 14.52% enabling Endpoint Privacy Zones (EPZs). Hybrid privacy configurations, where profiles are private but activities remain public, account for 25.4% of users. Complementary insights from the user study confirm this limited adoption and highlight key barriers: lack of awareness, low

CHI '26, Barcelona, Spain

ACM ISBN 979-8-4007-2278-3/2026/04
https://doi.org/10.1145/3772318.3791408

perceived necessity, concerns about reduced functionality, and difficulty navigating settings. Together, these results reveal both a structural and behavioral resistance to adopting available privacy protections.

This paper makes the following key contributions:

- **Systematic categorization of privacy features:** We provide a structured overview of the privacy controls in major fitness-tracking platforms, identifying similarities and differences in their design.
- **Empirical case studies:** Using Strava and Garmin Connect as case studies, we analyze 197,873 publicly available user records to quantify privacy features adoption and measurable privacy risks. The anonymized dataset we collect can serve as a reusable foundation for future research.
- **User study of privacy behaviors:** We complement the empirical analysis with a survey of 182 users, through which we measure the features that could not be assessed empirically and identify reasons for non-use for all available privacy features.

2 Fitness Tracking Platforms

With the widespread availability of wearable devices and sensors, everyday users can now record their physical activities while exercising. Users can further upload their fitness data to fitness-tracking platforms that allow them to track their performance, visualize their progress, and compete with or compare their performance to other users.

Platforms such as Strava [69], MapMyRun [48], and Garmin Connect [13] integrate social networking with performance analytics, transforming how users engage with fitness data. Among these, Strava and Garmin Connect are the most popular in terms of user base, with Strava reporting over 150 million registered users globally [71] and Garmin Connect being widely adopted among owners of Garmin devices. Considering the total number of devices sold and typical adoption rates, the platform estimates between approximately 60 and 105 million active accounts [45, 46].

These platforms collect sensor data from smartphones and wearable devices to monitor heart rate, step count, oxygen saturation, blood pressure, menstrual cycles, and sleep patterns. This information is used to generate performance summaries, activity trends, and detailed workout breakdowns. Unlike traditional social networks, these platforms are built around fitness-related interactions, such as activity sharing, challenges, and leaderboards. Users can follow friends, like and comment on workouts, and compete for rankings on defined portions of roads, trails, or paths called segments, typically ranging from a few hundred meters to several kilometers. When users upload GPS-tracked activities, the platform identifies portions of their route that overlap with these segments. This allows users to compare performance metrics, such as time, speed, or pace, on specific sections of commonly used routes.

Many platforms allow users to create their own segments from previously recorded activities. Each segment is defined by a start point, an endpoint, and a series of intermediate locations, meaning segments can only be generated from routes that already exist in the user's activity history [72]. Platforms often provide interactive maps where users can explore and search for segments, including popular or user-generated routes, to plan training or compete with others. Leaderboards rank users based on their best performance on each segment, typically separated by activity type such as running, cycling, or hiking. Leaderboards usually display details such as rank, athlete name, date of the activity, and performance metrics like time, pace, speed, or heart rate. Athlete names often link to users' profiles, allowing further exploration of their activity history.

Privacy Violations. While fitness-tracking platforms provide valuable tools for monitoring physical activity, they also pose significant privacy risks. Studies have revealed vulnerabilities that allow sensitive user data to be exploited.

Zhou et al.[86] evaluated FitLock, a proposed defense for Fitbit, and found critical flaws, including unencrypted tracker identifiers that allowed attackers to track users across sessions. More recent work has focused on location privacy. Meteriz et al.[50, 51] showed that elevation profiles alone can reveal users' workout routes, while Hassan et al.[33] found that 95.1% of Strava users were vulnerable to location inference despite Endpoint Privacy Zones. Dhondt et al.[17] further demonstrated that leaked distance metadata could reconstruct EPZs using regression analysis.

Fitness tracker data can also reveal personal attributes. Zufferey et al.[87] showed that step count and heart rate data could classify users by personality traits. Surma et al.[74] demonstrated membership inference attacks using step counts to infer gender, age, and education. Similarly, Hernandez-Acosta et al. [34] showed that smartwatch data from cycling activities could reveal bike type, seat height, gear selection, and terrain with 92-96% accuracy.

3 Related Work

Prior work in fitness-tracking and wearable platforms has examined privacy risks, user perceptions, and sharing behaviors. A systematic review has summarized privacy risks and research trends across a broad body of wearable studies [63], whereas survey- and interview-based studies have examined users' privacy awareness, perceptions, and sharing behavior, typically using samples of a few hundred participants, ranging from approximately 200 to 630 users [80, 81, 88]. In parallel, analyses of publicly shared fitness-tracking data have demonstrated actual risks such as location exposure, inference of sensitive routines, and unintended disclosure when data is linked across platforms [3, 16, 29, 42]. While these studies provide important evidence about privacy risks and exposure, they do not examine how often users actively configure available privacy features, nor do they assess such behavior at the scale enabled by large collections of activity data and complementary user studies. Our work addresses this gap by measuring how often privacy features are used in practice and by examining why users choose not to adopt them.

3.1 Privacy Behavior in Fitness-Tracking Platforms

In the literature, studies on fitness-tracking platforms have primarily examined users' perceptions of privacy risks rather than their actual behavior. Velykoivanenko et al. [81] conducted a longitudinal study with 227 participants and found that although users recognize potential privacy threats, they often underestimate risks and engage minimally with available privacy settings. While their work identifies awareness gaps, it does not measure real-world configuration choices; our study addresses this by quantifying actual adoption at scale. Theis et al. [80] similarly reported that privacy policies are rarely read or understood and that users prefer centralized, low-effort privacy controls, highlighting the role of usability barriers. We complement these findings by showing how such barriers manifest in concrete configuration patterns on Strava and Garmin Connect.

Other work has focused on privacy risks related to data sharing. Niksirat et al. [63] reviewed 236 studies on wearable activity trackers, emphasizing risks from sensitive inference and third-party access but noting a lack of empirical research on how users actually configure privacy protections. Our empirical measurements directly fill this gap. Zufferey et al. [88] examined Third-Party Application (TPA) ecosystems and found that users systematically underestimate the number of TPAs with access to their data and rarely revoke permissions, reinforcing concerns about user awareness and control.

To help explain these behaviors on fitness-tracking platforms, prior privacy research provides useful context. The privacy paradox describes gaps between users' stated privacy concerns and their actual behavior [40], a pattern that has been observed across many online platforms and motivates an examination of whether similar gaps appear in fitness-tracking settings such as Strava and Garmin Connect. Similarly, the privacy calculus suggests that users weigh perceived risks against perceived benefits when deciding whether to share information [18, 66, 85]. In the context of fitness-tracking platforms, this framework suggests that perceived benefits such as social interaction, competition, and convenience may outweigh privacy concerns, potentially leading to limited use of available privacy controls.

Usability also plays an important role. Prior work shows that complex interfaces, unclear settings, and non-transparent defaults can discourage users from adjusting privacy options [14]. Related studies further indicate that users may be unaware of available privacy features, have difficulty locating relevant settings, or lack the knowledge needed to configure them effectively. This aligns with broader findings that users may value privacy in principle but lack the ability or motivation to act on those concerns [9].

Together, these bodies of work reveal a disconnect between users' privacy intentions, their understanding of privacy risks on fitness-tracking platforms, and their actual engagement with available privacy tools. Our study advances the field by providing the first large-scale measurement of actual privacy-setting configurations on fitness-tracking platforms and by tying observed behavior to user-reported motivations.

3.2 Data Collection and User Practices in Wearable and Social Platforms

Wearable devices collect continuous, granular data, including location traces, movement patterns, physiological signals, and behavioral routines, that can reveal sensitive personal information. Prior research has shown that such data enables inference of home locations, daily routines, social relationships, and identities. Mobility traces are highly unique and re-identifiable [16], and home and work location pairs can reveal identity with high accuracy [29]. Krumm et al. [42] further demonstrated that location trajectories can expose sensitive attributes. These risks motivate our focus on whether users adopt protective features such as EPZs.

Research on fitness-tracking platforms has highlighted additional risks arising when activity traces are combined with publicly shared metadata. Aktypi et al. [3] showed that linking fitness-tracker outputs with social network information can reveal home locations and routines beyond what users intend to disclose. Our analysis builds on this work by examining whether users meaningfully employ available protections against such exposures. This highlights the need for usable and effective privacy controls, which we evaluate by measuring adoption and by studying users' reasons for non-use.

Privacy behavior on fitness platforms also aligns with longstanding findings in traditional social networks. Early studies on Facebook and X (formerly Twitter) showed that users rarely modified default privacy settings despite expressing concern about exposure [2, 31, 41]. More recent work indicates that this under-utilization persists even with more sophisticated interfaces [1, 15]. Our data shows that similar patterns appear in fitness platforms, with defaults strongly shaping behavior. Comparable trends have been documented on Instagram, X, and LinkedIn [20, 84], where public sharing remains common. Our empirical measurements examine whether similar tendencies toward public visibility also appear in fitness-tracking ecosystems.

By situating our findings within this broader literature, we show that fitness-tracking platforms reproduce many of the same behavioral challenges observed on social networks: users face significant privacy risks, value privacy in principle, yet rarely adjust defaults or engage with available protections. Our contribution is to provide concrete, at-scale evidence of this dynamic in the fitness-tracking domain and to identify which features are most affected.

4 Methodology

This study aims to address two key research questions related to privacy feature adoption in fitness tracking platforms: (Q1) *How many users of fitness tracking platforms use the available privacy features?* To answer this, we first develop a systematic categorization of privacy features across major platforms. We then perform a large-scale empirical analysis of publicly available data from Strava and Garmin Connect. By systematically analyzing adoption patterns across different categories of privacy controls, we establish a data-driven understanding of the actual use of these features in practice. (Q2) *What are the reasons behind users' adoption trends of privacy features in fitness tracking platforms?* While empirical measurements capture adoption rates, they cannot explain why users choose to engage or neglect these protections. To complement the quantitative analysis, we therefore conduct a user study in the form of an online questionnaire. The questionnaire targets individuals who actively use fitness tracking platforms and asks whether they adopt the privacy features we identify in our taxonomy (Table 1). For features not adopted, participants are invited to explain their reasons, allowing us to capture user perceptions, barriers, and motivations. The three components that synthesize our methodology, i.e., the privacy-feature categorization and empirical adoption measurement, and the user study, provide a mixed-methods approach that not only quantifies adoption at scale but also contextualizes the underlying factors shaping users' decisions about privacy on fitness-tracking platforms.

Ethical Considerations. This study received approval from our National Ethics Board for both the collection of publicly available data and the conduct of the user study. All data collected from Strava and Garmin Connect were strictly limited to information already publicly accessible through their public leaderboards and activity pages, in accordance with the platforms' terms of service. These publicly available records display non-private activity information such as leaderboard rankings, athlete and activity IDs, elapsed times, distances, pace, segment performance statistics, and, in the case of Strava, activity-stream data including GPS points, elevation, and accumulated distance that any logged-in user can view without special permissions. No private activities, restricted profiles, or data requiring elevated permissions were accessed. To mitigate any risk of deanonymization, all athlete identifiers and activity IDs were immediately pseudonymized using salted hashing and were never stored in plaintext. No usernames, profile descriptions, photos, or other personally identifying metadata were collected at any stage.

For the analysis of Reddit and Google Play reviews, we used only publicly posted comments and discarded all author-related metadata (e.g., usernames, timestamps, and URLs) at collection time, retaining solely the text required for thematic analysis.

All participants in the user study were fully informed about the purpose and procedures of the research and provided voluntary consent to participate. The survey was anonymous, collected no personally identifying information, and all responses were stored and analyzed only in aggregate form.

4.1 Categorization of Privacy Features

To provide a structured and consistent analysis, we developed a set of privacy feature categories using a systematic, multi-researcher approach. First, two researchers independently created user accounts on all six platforms and conducted a hands-on inspection of every settings menu, privacy configuration page, and account-management interface. Each researcher documented all privacy-relevant controls in a structured template capturing the feature name, menu path, available configuration values, and default settings. Both researchers also used each platform during regular activities (e.g., uploading workouts, editing profiles, joining challenges) to surface contextual privacy options that only appear during typical use. A third researcher then repeated the full inspection to validate completeness. All discrepancies across researchers were recorded, discussed, and resolved through consensus. This method follows similar methodologies used in prior HCI work on manual interface auditing and multi-coder validation [4, 30, 35, 43, 79]. Second, we consulted related work on privacy in fitness applications to identify recurring themes and standard categorizations [33, 38, 50, 51, 63]. This hybrid procedure results in a taxonomy grounded in real-world platform behavior and supported by prior research.

The taxonomy developed also serves as the foundation for our empirical analysis. Since no prior work provided a complete, cross-platform enumeration of privacy features, the manual documentation was necessary to establish the full feature space available across fitness-tracking platforms. This taxonomy allowed us to identify which privacy features exist in practice and, crucially, which of them could be measured using publicly accessible data. The full categorization of all features, along with the definition of each category, is provided in Section 5. In Section 6, we build directly on this categorization by assessing, for each feature in the taxonomy, whether it is directly observable (e.g., profile visibility), indirectly inferable (e.g., data-management features), or not measurable from public data (e.g., block/mute features). In this way, the taxonomy not only characterizes the landscape of privacy controls but also defines the scope and targets of our empirical data collection and analysis.

4.2 Empirical study

The primary objective of this study is to evaluate the adoption of privacy features by users of fitness-tracking platforms. To do so, we analyse publicly available data from Strava and Garmin Connect, focusing on how users engage with the privacy settings offered by these platforms.

We aimed to analyse the two largest categories of fitness-tracking ecosystems: (i) meta-networks that aggregate data from all major wearable devices, and (ii) device-based platforms tied to a specific wearable brand. For the first category, Strava is by far the largest meta-network, supporting data uploads from virtually all wearable brands and therefore offering the broadest and most heterogeneous user base, with over 150 million users worldwide [71]. For the second category, the largest device-based platform is Fitbit [57]. However, Fitbit does not maintain a public segment or leaderboard infrastructure, nor does it provide publicly accessible competitive records, which makes it incompatible with our empirical methodology that relies on segment-level public data. We therefore selected Garmin Connect, the second-largest device-based platform [45], which supports a public segment and leaderboard ecosystem comparable to Strava. By analysing Strava (the dominant meta-network) and Garmin Connect (the largest device-based platform with accessible segment data), our dataset captures key user groups from both major ecosystem types, offering a sample that is broadly reflective of the wider fitness-tracking landscape.

By analyzing publicly available leaderboard and activity data from these two platforms, we quantify the percentage of users adopting each privacy feature. Due to the nature of the available data, not all privacy features can be directly measured: some features can be inferred deterministically, others only indirectly, and some cannot be observed at all.

Data Collection. In this study, we collected only **publicly** accessible data, strictly adhering to the terms of service of both Strava and Garmin Connect, in line with standard practices commonly followed in similar research [17, 23, 33].

Our dataset includes 197,873 records obtained from public leaderboards on Strava and Garmin Connect, corresponding to frequently contested segments worldwide. From Strava, we collected data from eleven major segments spanning Europe, the USA, Canada, Australia, Asia, and Africa. From Garmin Connect, we included six widely used segments, primarily located in the USA and Europe. For activity privacy analysis, we randomly selected 10% of the activities from each crawled segment to ensure a geographically diverse and generalizable sample. This analysis was based on 19,200 individual activities linked to the Strava leaderboards. This sampling approach was necessary due to Strava's API limitations. Specifically, Strava's API restricts authenticated users to a maximum of 375 requests per day. As a result, the data retrieval process had to be carefully managed to ensure an efficient sampling while still capturing a robust and representative set of activities for the privacy analysis.

We used Selenium WebDriver [65] for automating the crawling process. For each segment, we visited the leaderboard page using the segment's unique ID, loaded the data page by page, and saved it in HTML format, which was then converted into a CSV file for analysis. The user IDs were pseudonymized by replacing them with hashed values and salt before storing the data. For each record in the leaderboard, we retrieved additional details such as the public activity IDs, activity times, pace, speed, and athlete IDs, when available, from the crawled leaderboard pages. For each activity ID, we first visited the corresponding activity page from `strava.com/activities/ID`, to extract the total distance. Additionally, for each activity, we retrieved the GPS track points, which included coordinate pairs, elevation, and accumulated distance data. This information was collected by visiting the activity streams page at `strava.com/activities/ID/streams`. We restricted this analysis to Strava, as Garmin Connect lacks an equivalent to Strava's `streams` endpoint, which provides detailed activity trace data.

To support transparency and reproducibility, the anonymized dataset used in this study is publicly available at https://bitbucket.org/srecgrp/fitness-networks-privacy-adoption-public.

4.3 User study

To complement the empirical analysis of publicly available data and address Q2, we conducted a mixed-methods user study in the form of an online questionnaire. Whereas the empirical analysis quantified actual adoption patterns, the survey explored both self-reported adoption of privacy features and the reasons for non-adoption.

The development of the questionnaire was directly informed by the findings of Sections 4.1 and 4.2. The manual documentation of privacy features provided a complete cross-platform list of available privacy controls, which we used to construct one survey item for each feature. This ensured that both features measurable in the empirical study and those that could not be inferred from public data were captured uniformly in the survey. In this way, the survey allowed us to obtain complete adoption information that complements the partial observability of the empirical dataset. The analysis of publicly available data also clarified which features are externally observable and which are not. This distinction guided our survey design: features that could not be measured in the empirical analysis were included to be captured through self-reported use, whereas observable features allowed us to compare self-reports against actual platform behavior.

The questionnaire was implemented in Google Forms and took approximately 5-10 minutes to complete. It combined closed-form multiple-choice and checkbox questions with one open-ended item, enabling the collection of both quantitative and qualitative data. The survey was fully anonymous, and no personally identifying information was collected beyond participants' responses to the study questions.

Participants were recruited through SurveySwap [76] and SurveyCircle [75], online platforms that allow researchers to exchange survey participation, as well as through personal contacts.

The questionnaire consisted of three main parts:

(1) Demographics and usage context: Participants reported their age group, education level, gender, and which fitness tracking platform they use. Additional questions addressed the type of information they provide to the platform (real, estimated, or fake), how often they use these platforms, and how important privacy is to them when using such apps.
(2) Feature-specific adoption: For each privacy feature listed in our taxonomy (Table 1), participants indicated whether they currently use it. If not, they were asked to specify their reasons for non-adoption by selecting one or more of the following options: I wasn't aware of it, I didn't think it was necessary, I didn't know how to change it, It limits the functionalities of the app (e.g., competition features, socializing), or Other (open text).
(3) General attitudes toward privacy: To capture broader perspectives, the survey concluded with an open-ended question: What would encourage you to use/adopt more privacy features in fitness tracking platforms?

Eligibility was restricted to individuals who reported actively using at least one fitness-tracking platform. We did not further limit participation to the six platforms analysed in Section 4.1, as these served as case studies for deriving a general taxonomy of privacy features rather than an exhaustive list of ecosystems. Survey items were based on these abstract feature categories (e.g., profile visibility, location protection), making them applicable across platforms. Restricting participation only to users of the six case-study platforms would have introduced unnecessary sampling bias without providing methodological benefits for Q2, which examines privacy-feature adoption in a platform-agnostic manner. Active use was assessed through self-report without additional verification, which is standard practice in online survey research. As an additional content-based indicator of respondent engagement and platform familiarity, the survey concluded with a required open-ended item. Meaningful responses to this item help indicate attentiveness and genuine experience with fitness-tracking applications, providing an indirect safeguard for data quality. All participants were informed about the purpose of the study and provided consent prior to participation. In total, we collected 182 valid responses.

We also note that placing demographic questions at the beginning of a survey can, in some contexts, introduce stereotype-threat effects [62]. Prior work shows that such effects occur mainly in surveys involving performance or evaluative tasks, such as math problems, where providing gender first led women to perform worse. In contrast, our questionnaire contained no tasks with right or wrong answers and asked only about participants' self-reported use of privacy features. As survey-methodology guidance indicates that demographic placement has minimal impact for non-sensitive, non-evaluative questions (e.g., factual self-reports like "How many gallons of milk did you purchase this week?") [62], we expect any stereotype-threat effects in our study to be negligible, though we acknowledge this as a methodological consideration.

Survey data were analyzed using Python, with pandas employed for data handling, matplotlib for visualization, and scikit-learn for statistical modeling and clustering. We adopted a mixed-methods approach that combined descriptive statistics, predictive modeling, unsupervised learning, and qualitative analysis.

First, descriptive statistics were performed to calculate adoption rates for each privacy feature, determine the relative prevalence of non-adoption reasons, and examine distributions across demographic groups. As part of these descriptive analyses, chi-square tests of independence [49] were conducted to assess whether privacy importance was associated with the adoption of specific features. To explore relationships between demographics, privacy attitudes, and adoption, we applied logistic regression [36] from predictive modeling to model the likelihood of adopting specific privacy features.

To identify hidden structures in adoption behavior, we employed two unsupervised learning techniques: principal component analysis (PCA) for dimensionality reduction [39] and k-means clustering to group respondents with similar adoption patterns [32]. These unsupervised methods revealed latent factors and clusters that are not visible through descriptive statistics alone.

Finally, qualitative data from open-text responses (both "Other" answers and the concluding open-ended question) were analyzed using thematic analysis [10]. The coding was conducted by one researcher using an iterative process to ensure consistency, beginning with open coding to capture recurrent ideas and followed by successive refinement into higher-level themes. Interim coding decisions and theme boundaries were discussed with the broader research team to ensure conceptual clarity and alignment with the study's aims. This combination of statistical modeling, unsupervised analysis, and thematic interpretation enabled both a broad overview of adoption and non-adoption patterns, and a deeper exploration of the motivations influencing user behavior in fitness tracking platforms.

5 Privacy Features in Fitness Tracking Platforms

The vulnerabilities identified in these platforms show how sensitive user data, such as location and activity metrics, can be exploited by adversaries. As a result, the need for robust privacy controls is crucial in these networks. Building on the categorization process introduced in Section 4, we now present the full taxonomy of privacy features identified across major fitness-tracking applications. The categorization is based on our systematic inspection of Strava [68, 70], Garmin Connect [27, 28], MapMyRun [5, 6], Fitbit [21, 22], Nike Run Club [54, 55], and Runkeeper [7, 8], and serves as the foundation for the empirical and survey analyses that follow.

The final categories include: *User Profile Controls*, *Activity Privacy*, *Location Protection*, *Data Management*, and *Social and Community Settings*. Categories such as *User Profile Controls*, *Activity Privacy* and *Social and Community Settings* were primarily derived from our direct interaction with the platforms, as they reflect how users configure the visibility of their profile and manage interactions with others. In contrast, categories including *Location Protection* [33, 38, 50, 63], and *Data Management* [63] are strongly grounded in prior work, which emphasizes the risks associated with exposing activity data, disclosing location traces, and handling sensitive personal information.

The rest of this section provides a detailed description of the identified privacy features.

5.1 User Profile Controls

This category covers features that regulate how a user's identity and personal information are exposed, as well as how they interact with others on the platform. Profile visibility settings allow users to define the accessibility of their personal details, typically offering options that range from fully public, to limited to approved connections, to entirely private. Some platforms also provide photo privacy settings, enabling users to manage who can view images associated with their profile. Blocking and muting features give individuals control over unwanted interactions, while Youth protections apply stricter default settings for underage users, limiting both data visibility and opportunities for public interaction.

5.2 Activity Privacy

This category includes controls that determine the visibility of individual or overall user activities. Platforms typically provide options that range from fully public, to restricted to approved connections, to completely private. In some cases, users can adjust visibility on a per-activity basis, while others apply global privacy settings across all activities. Participation in community features such as leaderboards or challenges is generally limited to publicly visible activities, with private activities excluded from rankings and competitive features.

5.3 Location Protection

To address sensitive location privacy, platforms offer Endpoint Privacy Zones (EPZs), which allow users to hide sensitive parts of their activity routes, such as those near their home or workplace. Although users can still share activities with EPZs, the hidden segments are excluded from performance comparisons.

Users can define EPZs around multiple sensitive locations, with each location having one zone. Only the activity owner can see the full route, while others see a masked version where the start and end near EPZs are hidden. Different platforms implement EPZs with varying settings. For example, Strava uses circular zones with radii from 200 to 1,600 meters (in 200-meter steps), while Garmin Connect offers 100 to 1,000 meters (in 100-meter steps), affecting how users manage their privacy [19]. Figure 1 illustrates how an activity appears to its owner when an EPZ is applied (Figure 1a) and how it is displayed to other users (Figure 1b).

5.4 Data Management

This category encompasses user autonomy over personal information. Data Export/Deletion features allow users to download or permanently erase their data. Third-party Access Management provides fine-grained control over which external applications may access health or activity data.

5.5 Social and Community Settings

This category includes features that regulate users' participation in social interactions and community activities while preserving

Table 1: Privacy Features Categorized Across Fitness Platforms

Privacy Feature Category / Feature	Strava [68]	Garmin Connect [28]	MapMyRun [5]	Fitbit [22]	Nike Run Club [54]	Runkeeper [8]
User Profile Controls						
Profile Visibility	✓	✓	✓	✓	✓	✓
Blocking/Muting Users	✓	✓	✓	-	✓	-
Youth Protections	✓	-	-	-	-	-
Activity Privacy						
Activity Visibility	✓	✓	✓	-	✓	✓
Location Protection						
Start/End Point Obfuscation (EPZ)	✓	✓	✓	-	-	✓
Route Visibility Restrictions	✓	✓	✓	-	-	✓
Data Management						
Data Export/Deletion	✓	✓	✓	✓	✓	✓
Third-party Access Management	✓	✓	✓	✓	✓	✓
Social and Community Settings						
Hybrid Privacy Mode	✓	✓	✓	-	✓	✓
Challenge Participation Controls	✓	-	-	-	-	-

privacy. We define *hybrid privacy mode* as a combination of privacy features in which users maintain a restricted or limited profile, while making some or all of their activities public. This allows users to compete in challenges, appear on segment leaderboards, or participate in community events without fully exposing their personal profile information. By enabling this combination of settings, hybrid privacy mode provides flexibility for balancing social engagement with personal privacy.

Some platforms, such as Strava, explicitly allow users to hide activities from public leaderboards during challenges, enabling private participation while still engaging competitively. Other platforms, including Garmin Connect, Nike Run Club, MapMyRun, RunKeeper, and Fitbit, provide activity privacy controls, but do not offer a dedicated option to participate in challenges or leaderboards privately. Table 1 summarizes which platforms support each of these privacy features.

6 Empirical Study Results

In this section, we analyze the adoption and usability of the privacy features identified in Section 5. For our empirical measurements, we use the Strava and Garmin Connect platforms as case studies. However, following the categorization in Table 1 that reflects a broader set of features found across multiple fitness platforms, including MapMyRun, Fitbit, Runkeeper and Nike Run Club, our methods and findings can be applied to other fitness platforms as well, offering broader insight into privacy practices across the ecosystem.

We categorize the identified features based on their availability for analysis into three groups: (i) Directly Measurable, which refers to features whose usage can be directly observed from public data; (ii) Implicitly Measurable, where the adoption of the feature can be inferred indirectly through probabilistic methods or inferences; and (iii) Not Measurable, which includes features for which no data is available for direct or inferred measurement due to platform restrictions or lack of observable indicators. Table 2 presents the category in which each feature belongs. Features such as Blocking/Muting and Youth Protections are classified as *Not Measurable* because these actions occur privately between users and are not exposed by the platforms for external analysis.

To ensure accuracy and reliability, we limit our evaluation to features that can be directly or indirectly measured using publicly available data from Strava and Garmin Connect, except for location privacy, which we evaluate only on Strava, due to platform limitations we mention in Section 4.2. Thus, we provide a clear picture of which privacy features Strava and Garmin Connect users actually use. Furthermore, this is the first study to systematically examine the real-world use of privacy controls on fitness-tracking platforms at scale. By analyzing patterns of feature adoption, we reveal previously unexplored trends and potential privacy risks resulting from how users engage, or fail to engage, with available protections.

6.1 Profile Visibility

In this section, we examine how many users in our dataset employed profile-level privacy controls, including settings that restrict the visibility of profile photos. In these platforms, profile photo visibility is inherently coupled with overall profile visibility, as private profiles limit photo access to followers by default.

Table 4 presents the percentage of private accounts in public leaderboards, while Figure 2 illustrates the percentage of private profiles per segment. The percentage of private accounts varies across different regions. Europe has the highest percentage of private accounts at 39.6%, followed closely by the USA at 38% and Japan at 37.8%. South Africa reports a moderate percentage of 29.5%, while Canada and Australia show lower values at 28.3% and 26.5%, respectively. Overall, the percentage of private accounts for all regions ranges from 26% to 39.6%. To better understand the trend across all segments geographically and ensure a more accurate comparison, we calculate the average percentage of private accounts. The average private account percentage across all segments is 36.4%. This suggests that since most segments have private account percentages in the mid-to-low thirties, the total usage of this privacy feature is not very high, as it does not even rise to 50% across most segments. In fact, the relatively low percentages indicate that a significant proportion of users are either not using this feature or prefer to

Table 2: Classification of privacy features based on their measurability

Privacy Feature Category / Feature	Directly Measurable	Implicitly Measurable	Not Measurable
User Profile Controls			
Profile Visibility	✓		
Blocking/Muting Users			✓
Youth Protections			✓
Activity Privacy			
Activity Visibility	✓		
Location Protection			
Start/End Point Obfuscation (EPZ)	✓		
Route Visibility Restrictions			✓
Data Management			
Data Export/Deletion			✓
Third-party Access Management		✓	
Social and Community Settings			
Hybrid Privacy Mode	✓		
Challenge Participation Controls		✓	

Table 3: Summary of Privacy Feature Usage Across Categories

Category / Feature	Adoption Percentage
User Profile Controls	
Profile Visibility	36.42%
Activity Privacy	
Activities Utilizing Extra Feature (Activity Hiding)	2.12%
Location Protection	
Start/End Point Obfuscation (EPZ) Usage	14.52%
Social and Community Settings	
Hybrid Privacy Mode Usage	25.40%

Table 4: Total number of activity records and percentage of private accounts

Segments' area	Total Number of Records	Percentage of Private Accounts
USA	39,495	38%
Australia	22,329	26.5%
Europe	59,910	39.6%
South Africa	9,864	29.5%
Canada	34,100	28.3%
Japan	23,024	37.8%

keep their accounts public. The fact that no Strava segment reaches even a 50% usage rate suggests that privacy concerns may not be a top priority for the majority of users across these regions. However, Garmin Connect's segments show a different trend, with many of them either very close to or exceeding 50% usage, indicating that privacy settings are more widely adopted among Garmin users.

6.2 Activity privacy

Only activities set to public appear in public segment leaderboards. While 197,873 such activities were collected from 17 segments across two fitness platforms, this dataset reflects only publicly visible activities. Users are not required to make all their activities public to participate in leaderboards; visibility can be configured on a per-activity basis. As such, the appearance of an activity in a leaderboard does not indicate a user's overall privacy preferences or default settings. Our findings, are based solely on this publicly available subset.

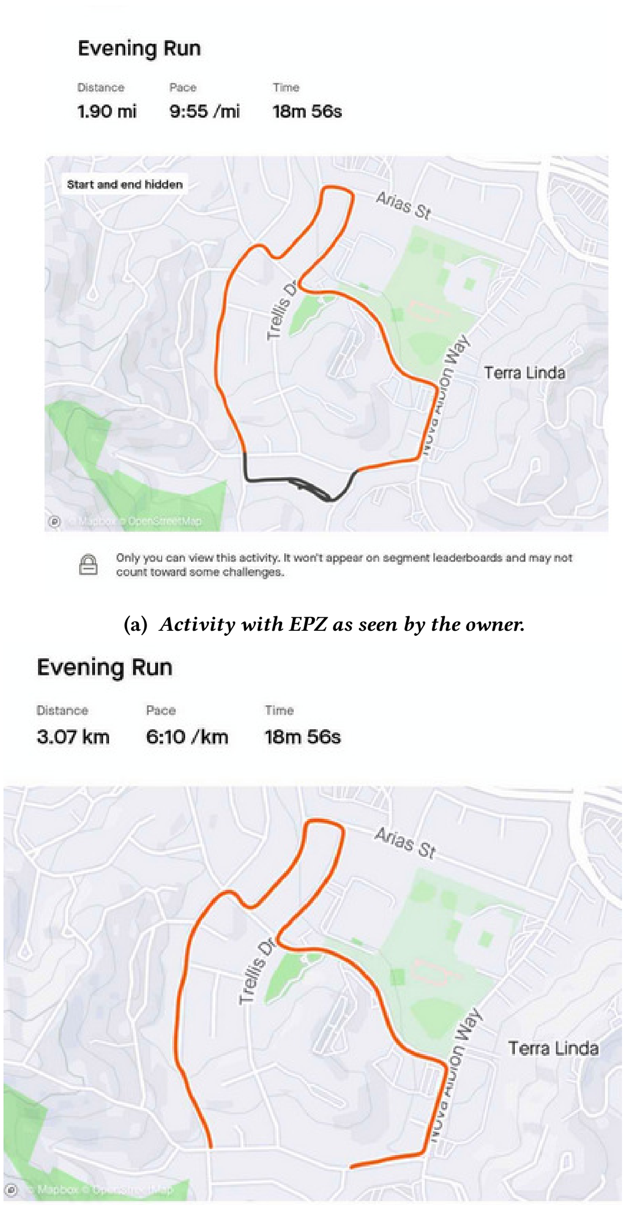
However, Strava offers users the ability to selectively hide specific components of their activities, such as the map, heart rate and elevation data, providing more granular control over the visibility of their activity details. In contrast, Garmin Connect does not offer this level of customization, as users can only limit the visibility of the entire activity. Given this difference, we will measure the usability of this feature across the 192,803 activities from Strava.

From the total of 192,803 records, we randomly selected 10% of the activities from each segment to ensure that the sample was geographically diverse and could be generalized to represent the broader activity trends across the different regions. This approach led to a final sample of 19,200 individual activities linked to the Strava leaderboards, providing a balanced representation from each segment. The random sampling process was essential for ensuring that our analysis covered a wide range of activities across the world, despite the limitations imposed by Strava's API.

Table 3 presents the results of the activity privacy analysis. We observe that, out of the total 19,200 individual activities, only 465 utilize the additional feature to hide certain parts of the activity, resulting in a usage rate of 2.12%. This low usage rate indicates that the feature is either not widely adopted or that users do not perceive a strong need to obscure specific parts of their activities. It could also suggest that users are not fully aware of the feature's existence, limiting their ability to use it.

6.3 Hybrid privacy mode

To measure the adoption of the hybrid privacy mode in fitness-tracking platforms, we calculate the number of users who have set their profile to private while still participating in public leaderboards. Since our data is collected from public leaderboards on both Strava and Garmin Connect, we use the athlete IDs provided there to visit each user's profile. This step is required because the privacy setting is not visible in the leaderboard itself and can only be determined from the user's profile page. We then classify each account



Evening Run

Distance 1.90 mi

Pace 9:55 /mi

Time 18m 56s

Start and end hidden

Only you can view this activity. It won't appear on segment leaderboards and may not count toward some challenges.

(a) *Activity with EPZ as seen by the owner.*

Evening Run

Distance 3.07 km

Pace 6:10 /km

Time 18m 56s

(b) *Activity with EPZ as seen by others.*

Figure 1: Comparison of EPZ visibility for owner and other users [73].

accordingly and compute the percentage of private accounts for every segment’s leaderboard.

Table 3 presents the results of the hybrid privacy mode usage analysis. Out of a total of 197,873 activities, 50,262 activities were conducted with the hybrid mode. This indicates that while 25.4% of users choose to set their profiles to private, they still make their activities publicly available, to maintain participation in public leaderboards.

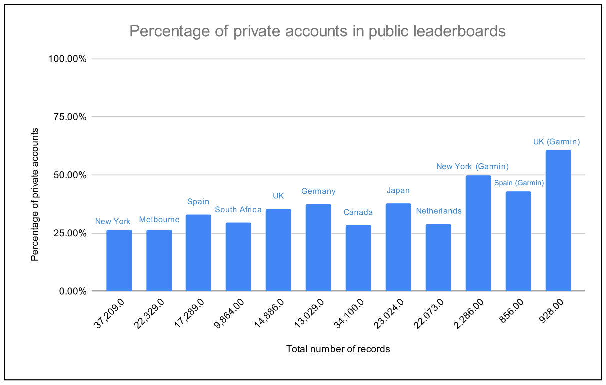


Figure 2: The figure above shows the percentage of private accounts in each publicly available leaderboard for both Strava and Garmin Connect segments.

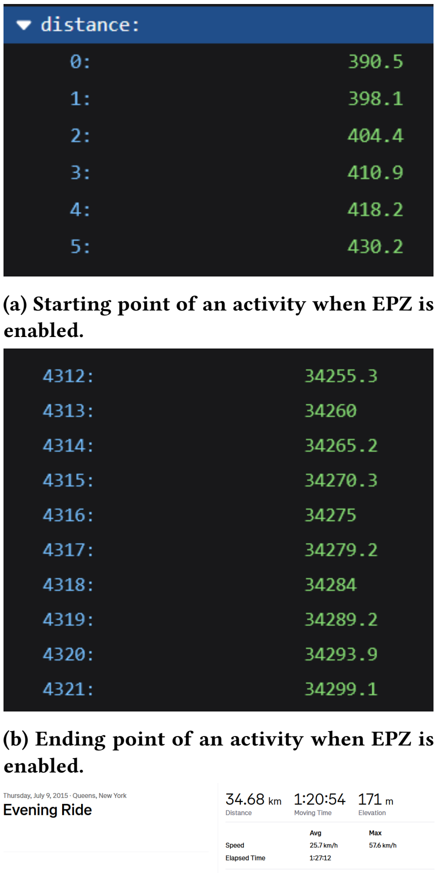
6.4 Location Privacy - EPZ

Endpoint-Privacy Zones (EPZs), allow users to obscure only the start and/or end of their route, as described in Section 2. Dhondt et al. [17] demonstrate that EPZ implementations are still vulnerable to inference attacks, by exploiting distance information in activity metadata. In their paper, they also presented methods for identifying activities that use the EPZ functionality.

We apply the detection method presented in [17] to measure the adoption of EPZs in fitness tracking platforms. To achieve this, we must collect both the total distance of each activity in our dataset and its corresponding stream. A stream in Strava is a dataset that provides detailed, sequential data points for various attributes of an activity. Essentially, it is a time-series dataset that records various attributes of an activity, such as GPS coordinates (latitude and longitude), elevation, speed, and other metrics at regular intervals. This data is primarily used to generate the activity map on the Strava platform, allowing users to visualize their routes in detail. Each recorded point in the stream contributes to reconstructing the path taken during the activity, enabling accurate distance and elevation calculations. Moreover, Strava `stream` data is formatted as JSON.

Each set in the JSON file, such as “surface”, “moving”, and “distance”, contains the corresponding data points recorded at regular intervals throughout the activity. The only dataset of interest in our work is “distance”. The distance set in the file represents the cumulative distance covered during an activity, measured in meters. Each value corresponds to a recorded point in the activity stream, showing the total distance covered from the starting point up to that specific moment.

As acknowledged in [17], while points inside the EPZ are hidden, the total distance of the activity and the accumulated distance for the visible segments remain unchanged. This difference results in a mismatch between the accumulated distance points in stream files and the total distance displayed on the activity page. More specifically, activities that use EPZ have a first distance point that is not 0.0 meters in the stream file, and the last distance point is smaller than the total activity distance. Figure 3a shows the starting distance of an activity and Figure 3b shows its last distance point, while the total distance of the activity is represented in Figure 3c. The activity starts at 390.5 meters and ends at 34,299.1 meters. However, the total distance of the activity is 34.68 km, which equals to 34,680 meters. This difference in total distance, along with the fact that the activity starts at 390.5 meters instead of 0.0, indicates that the owner of the activity has utilized an EPZ. To quantify EPZ adoption, we retrieved each activity's total distance from its activity page and collected the corresponding JSON from the streams page. Table 3 records the results of our analysis. Out of 19,200 total activities analyzed, 9,552 utilized EPZs, representing 14.52% of all activities.



```
▾ distance:
    0:        390.5
    1:        398.1
    2:        404.4
    3:        410.9
    4:        418.2
    5:        430.2
```

(a) Starting point of an activity when EPZ is enabled.

```
4312:    34255.3
4313:    34260
4314:    34265.2
4315:    34270.3
4316:    34275
4317:    34279.2
4318:    34284
4319:    34289.2
4320:    34293.9
4321:    34299.1
```

(b) Ending point of an activity when EPZ is enabled.

Thursday, July 9, 2015 · Queens, New York

Evening Ride

34.68 km	1:20:54	171 m
Distance	Moving Time	Elevation

	Avg	Max
Speed	25.7 km/h	57.6 km/h
Elapsed Time	1:27:12	

(c) Total distance of the activity from the activity's page.

Figure 3: Representation of the mismatch between the distance points when activities fall into EPZs.

6.5 Challenge Participation

Strava challenges let athletes set goals, track progress, and compete with others. While all participants can earn badges and rewards, only activities set to public appear in the public leaderboard. Strava's privacy settings allow users to hide their activities from the leaderboard, meaning not all participants are visible. To measure how many users adopt these privacy settings, we analyzed 10 active public challenges, comparing the total number of participants to those appearing in the leaderboard. In every case, the leaderboard had fewer athletes than the total participants.

This means participants missing from the leaderboard either did not complete a qualifying activity or used privacy settings to keep their activities private. While we cannot tell why each individual is absent, we can say that the athletes in the leaderboard did not use privacy settings for challenge participation. Comparing the leaderboard size to the total participants gives us a minimum estimate of how many athletes chose not to make their activities private.

Table 5 presents the analyzed Strava challenges, along with their total number of participants and the number of leaderboard participants. The last column shows the calculated percentage of public activities based on leaderboard participation. Next, we calculate the average percentage of public activities across all challenges. The average percentage of public activities in Strava challenges is 63.4%. After calculating the average, we cannot definitively determine how many participants used the privacy feature. However, based on the data, we can conclude that 63.4% of the total participants across all challenges (3,997,960 participants) did not use the feature (i.e., their activities were publicly visible). In the best-case scenario, where all participants who did not appear on the leaderboard used a privacy feature for activity visibility in the challenge (without considering participants who did not complete the challenge or reach the goals), the adoption rate for privacy features would be *at most* 36%.

6.6 Data Management

6.6.1 Methodology. To analyze data-management feature adoption in fitness tracking platforms, we employed an NLP-based approach consistent with prior work on privacy discussions in online ecosystems [53, 77, 78]. We collected Reddit discussions using the PRAW API [61] between March and April 2024. Posts and comments were retrieved from subreddits such as `r/fitness`, `r/Strava`, `r/Garmin`, `r/Fitbit`, and `r/MapMyRun` using the single keyword "permissions" to identify relevant threads. In parallel, we extracted publicly available Google Play Store reviews for major fitness-tracking applications, including Strava, Garmin Connect, Fitbit, Runkeeper, and Nike Run Club.

Text data were pre-processed by removing stop words, punctuation, and non-textual characters. After retrieval, we identified permission-related mentions using the set of regular-expression patterns implemented in our analysis script, which capture phrases involving the granting or allowing of access (e.g., patterns matching combinations of *allow*, *grant*, *consent* with *granted permission*, *allow access*, *I agreed to*, or *shared data*). We then applied thematic analysis [10] to group these mentions into recurring themes related to data access and third-party sharing, supplemented by word-frequency analysis to highlight dominant terms in user discourse.

6.6.2 Results. A total of 1,066 Reddit posts and app reviews were analyzed. Of these, 67.35% of user comments explicitly mentioned granting permission or allowing data-sharing with third parties. The most frequently used words in permission-related discussions included "permission" (405 occurrences), "data" (389 occurrences), and "access" (91 occurrences). Many users expressed concerns over the extent of data access required by fitness applications, often questioning the necessity of certain permissions. There was also

Table 5: Percentage of publicly visible activities in Strava challenges.

Challenge	Total participants	No. of Leaderboard participants	% of Public Activities
February Run 300K	311,256	235,136	75.54%
February Cycling Elevation	269,584	202,187	75%
February Gran Fondo	344,342	93,576	27.2%
February Ride 800K	273,495	210,827	77.1%
February Walk 50K	510,094	293,684	57.6%
February Snowsport	152,531	42,286	27.8%
February 400-minute	1,216,208	959,297	78.9%
February Ride 200K	517,847	382,203	73.8%
February 5K	1,314,972	834,047	63.4%
February Elevation	482,188	364,010	75.5%

a notable pattern of users discussing third-party integration and how data-sharing policies affected their trust in fitness tracking platforms.

While these findings indicate that a significant portion of users acknowledge and grant permissions, they do not confirm whether users actively change the default settings or simply accept the permissions as presented by the app. It is important to note that this measurement is implicit, meaning it relies on user discussions rather than direct behavioral data. As a result, it is a probabilistic estimation rather than a definitive measure of user engagement with data management settings.

The findings from our analysis of app reviews and Reddit posts, where 67.35% of users explicitly mentioned granting permission or allowing data-sharing, align with the results of Zufferey et al. [88], who found that 70% of fitness tracker users shared their data with at least one third-party application. This consistency suggests that both user discussions and survey-based approaches yield similar insights into user behaviors regarding data-sharing permissions.

7 User Study Results

To complement our empirical analysis, we conducted a user study to understand perspectives on privacy features in fitness platforms. Our goal was to verify adoption levels and, most importantly, uncover why many users do not adopt these protections. This section introduces our participants, reports adoption rates, examines reasons for non-use, presents statistical and clustering analyses that contextualize these behaviors, and concludes with factors that might encourage adoption.

7.1 Participant Overview

The survey was open to any individual using fitness tracking platforms, and participation was based on a random sample of users willing to respond to the questionnaire. A total of 182 participants completed the survey, and their demographic and background characteristics are summarized in Table 6.

Our sample size, $n = 182$ provides sufficient statistical power for the analyses employed in this study. For χ^2 tests and logistic-regression models predicting privacy-feature adoption, conventional guidelines on events-per-variable (EPV) recommend roughly 5-10 outcome events per predictor variable to yield stable estimates and avoid overfitting [60, 83]. Given our observed outcome frequencies and the limited number of predictors, our study meets these EPV thresholds. Moreover, classical power-analysis frameworks for social and behavioural research suggest that a sample of this size is adequate to detect medium to large effects at conventional significance levels [12]. Also, similar sample sizes have been used in prior work employing logistic and chi-square analyses to model privacy-related behaviours. For instance, ordered logistic regression has been applied with samples of around 178 participants to study privacy and security-setting use [24], and multinomial logistic regression has been used with approximately 150 fitness-tracker users to examine trust and adoption patterns [52]. Likewise, chi-square tests have been used with samples near 180 participants to analyse privacy-related choices and functional differences [44]. Together, these studies demonstrate that logistic- and chi-square-based analyses in privacy and wearable-technology contexts are commonly conducted with sample sizes comparable to our $n = 182$.

Table 6: Participant demographics and usage characteristics ($n = 182$).

Category	Group	Percentage (%)
Gender	Female	62.2
	Male	34.4
	Prefer not to say	3.3
Age group	18–24	34.8
	25–34	38.8
	35–44	18.0
	45–54	6.7
	55+	1.7
Education	Primary school	1.1
	Secondary school	7.9
	Bachelor's degree	38.4
	Master's degree	43.5
	Doctorate/professional degree	9.0
Privacy importance	Not important	6.7
	Slightly important	20.2
	Neutral	17.4
	Important	23.0
	Very important	32.6
Frequency of use	Daily	28.1
	Several times a week	38.8
	Weekly	13.5
	Less than weekly	19.7
Type of information shared	Actual personal information	76.7
	Estimation of real information	17.6
	Fake information	5.7
Platform usage	Strava	36.4
	Fitbit	30.7
	Garmin Connect	20.0
	Nike Run Club	14.8
	Apple Fitness	9.1
	Samsung Health	2.3
	Runkeeper	1.7

Beyond these statistical considerations, our sample size is also well aligned with empirical norms in fitness-tracking and wearable-privacy research. Prior studies in this space report comparable sample sizes, including Gabriele and Chiasson's survey examining users' privacy attitudes and behaviours in fitness-tracking platforms (212 participants) [26], Vitak et al.'s study of privacy attitudes and data valuation among fitness-tracker users (361 participants) [82], and Cho et al.'s analysis of privacy-related disclosure and continuance decisions in wearable-device use (248 participants) [11]. Even foundational qualitative work in this domain, such as Fritz et al.'s investigation of long-term behaviour and engagement with activity-tracking devices, relies on smaller but deeply contextual samples (30 participants) [25]. Collectively, these examples show that our sample of 182 participants fits well within the established range of empirical studies examining privacy, behaviour, and user practices in fitness-tracking contexts.

The sample was composed of a majority of female respondents (62.2%), with male participants accounting for 34.4% and 3.3% preferring not to disclose their gender. In terms of age distribution, the largest groups were 25–34 years (38.8%) and 18–24 years (34.8%). Participants aged 35–44 years represented 18%, while 45–54 years and 55 years or older were less represented (6.7% and 1.7%, respectively). The education profile of respondents was skewed towards higher education. Over two-thirds held a university degree, with 43.5% reporting a Master's degree and 38.4% a Bachelor's degree. In addition, 9.0% held a doctorate or professional degree (e.g., PhD, MD, JD). Only 7.9% reported secondary school as their highest qualification, and a small minority (1.1%) indicated primary school education.

Participants were also asked about the importance of privacy when using fitness tracking applications, with response options ranging from *Not important*, *Slightly important*, *Neutral*, *Important*, to *Very important*. The distribution showed that most respondents considered privacy to be highly relevant, with 32.6% rating it as very important and 23% as important. A further 20.2% selected slightly important, 17.4% were neutral, and 6.7% regarded privacy as not important.

In addition to demographics and privacy perceptions, the survey examined platform usage, activity frequency, and data-sharing practices. The distribution of platform usage is illustrated in Figure 4. The most commonly used platform was Strava (36.4%), followed by Fitbit (30.7%), Garmin Connect (20.0%), Nike Run Club (14.8%), and Apple Fitness (9.1%). Less frequently mentioned platforms included Samsung Health (2.3%) and Runkeeper (1.7%). These findings from our user study further validate our selection of Strava and Garmin Connect as case study platforms. In terms of frequency of engagement, 28.1% of participants reported using fitness platforms daily, 38.8% several times a week, 13.5% weekly, and 19.7% less than once per week. When asked about the type of information shared on these platforms, the majority (76.7%) reported sharing actual personal information. A smaller portion (17.6%) provided estimations of their real data (e.g., approximate rather than exact details), while only 5.7% admitted to supplying entirely false information.

Overall, the sample reflects a young, highly educated group of fitness tracking users, with the majority emphasizing the importance of privacy, engaging regularly with multiple platforms, and typically sharing authentic personal information.

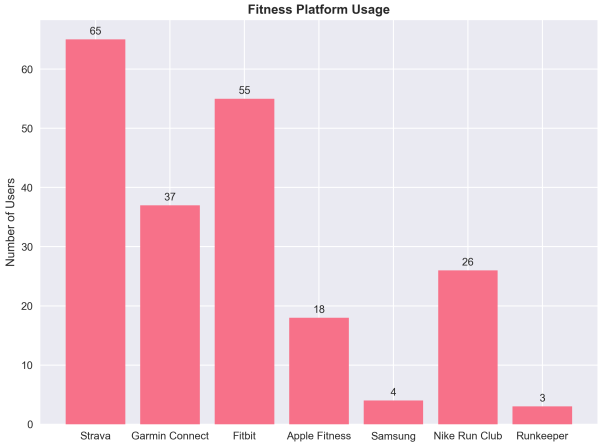


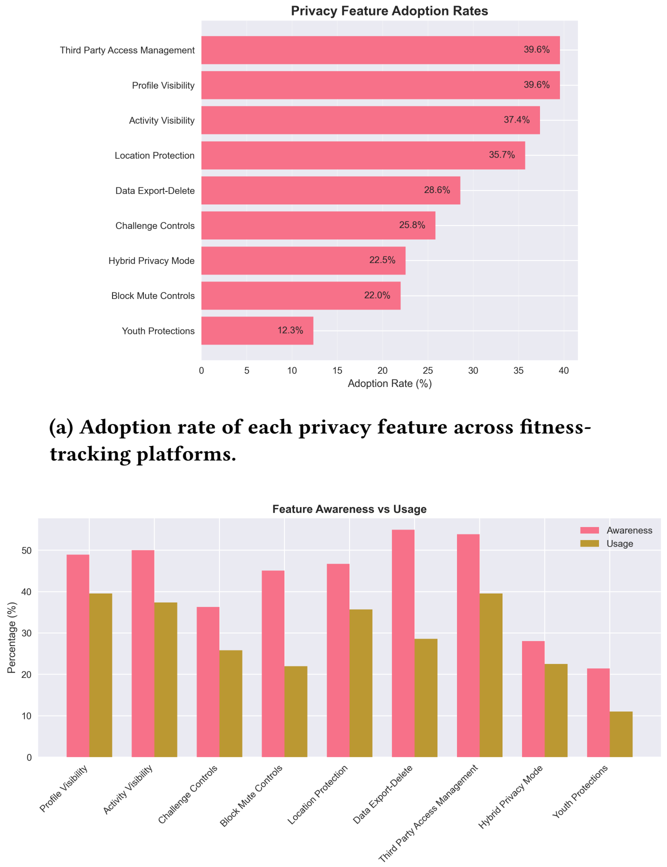
Figure 4: *Distribution of platform usage*. The figure shows how many survey participants reported using each fitness platform.

7.2 Adoption of privacy features

Figure 5a presents the adoption rates of the privacy features among survey participants. Overall, uptake was limited but non-negligible, with adoption concentrated in a handful of core controls. The most widely used features were profile visibility (39.6%), third-party access management (39.6%), and activity visibility (37.4%). Location protection mechanisms such as EPZs and route restrictions were reported by 35.7%, while data export and deletion tools were adopted by 28.6%. More specialized or situational controls saw lower uptake: challenge participation controls (25.8%), block/mute controls (22.0%), and hybrid privacy mode (22.5%). Youth protections were the least adopted at just 12.3%.

Figure 5b contrasts awareness with actual use. For every feature, awareness outstripped adoption, though the gap varied by category. The smallest discrepancies appeared for profile and activity visibility, where many respondents both knew about and used the controls. Larger gaps were evident for data export and delete management, block/mute controls, and third-party access, where users were aware of the settings but far fewer acted on them.

Figure 6 focuses specifically on users who rated privacy as important or very important, highlighting the adoption gap among those who were aware of each feature. The results indicate that awareness alone does not guarantee adoption, with sizeable gaps persisting for nearly all features. The most pronounced discrepancies were observed for youth protections (53.8%), data export and deletion (48.3%), and block/mute controls (48.1%), suggesting that even motivated users struggle to act on these settings. By contrast, visibility controls (profile and activity) showed smaller but still notable gaps of around 25–32%, while location protection (18.2%) and hybrid privacy mode (13.3%) had the lowest gaps. These findings underscore that the challenge is not simply a lack of awareness, but also barriers to translating awareness into consistent usage, particularly for complex or more specialized features.



(a) Adoption rate of each privacy feature across fitness-tracking platforms.

(b) Relationship between user awareness of each feature and their actual usage.

Figure 5: Adoption rates and the relationship between awareness and usage of privacy features in fitness-tracking platforms. The layout has been adjusted to improve readability by placing the plots vertically, increasing available space for labels and simplifying visual presentation.

7.3 Reasons for Non-Adoption

Participants who reported not using privacy features were asked to indicate their main reasons. The questionnaire provided four predefined options (*I wasn't aware of it*, *I did not think it was necessary*, *It limits the functionalities of the app (e.g., competition features, socializing)*, and *I did not know how to change it*). In addition, an open-ended "Other" option allowed participants to provide free-text responses. We conducted a thematic analysis [10] of these answers, which resulted in two further categories: *I do not interact with other users* and *I do not care*.

The distribution of all reported reasons is shown in Figure 7. The analysis of the reasons that affect users' decisions not to adopt privacy features is a collective assessment of all features. Crucial factors, such as lack of awareness and the perceived importance of privacy, can influence overall feature adoption, particularly for more specialized features. For example, if a user is unaware of a basic feature like profile visibility, they are also unlikely to adopt more specialized features such as hybrid privacy mode. The most frequent barrier was *lack of awareness*, reported 754 times across unused features. The second most common reason was *I did not think it was necessary* (367 mentions). Fewer responses indicated *functionality concerns* (129 mentions) or *I did not know how to change the settings* (87 mentions). Thematic analysis of the open-text responses [10] identified two additional categories: *I do not interact with other users* (14 mentions; for example, "I don't interact with anyone in the app" and "Don't interact with others") and *I do not care* (1 mention; "I don't care"). Because these counts are aggregated across all features, the frequencies exceed the total number of respondents.

Overall, the results suggest that non-adoption was dominated by *lack of awareness* and the perception that privacy controls were *not necessary*, while fewer mentions related to *functionality concerns*, *difficulties in changing settings*, or the perception that privacy controls were irrelevant because participants *do not interact with other users* or *do not care* about privacy.

7.4 Statistical Associations

Logistic Regression Analysis. We used logistic regression to examine predictors of adoption for each privacy feature, modeling the binary adoption outcome (e.g., profile visibility, activity visibility, challenge controls) as the dependent variable. Predictors included demographic factors (gender, age group, education), platform usage flags (Strava, Garmin, Fitbit, Apple Fitness), and survey responses on privacy importance, frequency of use, and information sharing.

Results indicate that platform usage was the most consistent predictor. Strava and Garmin Connect users were more likely to adopt features such as profile and activity visibility, whereas Apple Fitness usage was often associated with lower adoption. Demographic and attitudinal factors also contributed. For example, education and gender influenced activity visibility, and information-sharing preferences and age group affected adoption of data export-delete and youth protections. Model accuracies ranged from 0.60 (e.g., activity visibility, third-party access management) to 0.85 (youth protections), where higher accuracy suggests stronger and more systematic predictors of adoption, and lower accuracy indicates that adoption may depend on factors not captured in our model.

The full regression results, including top predictors and their directions of association, are visualized in Figure 13 in Appendix A.

Adoption by Privacy Importance and Chi-Square Analysis. Figure 8 shows that participants who consider privacy more important tend to enable a greater number of privacy features overall. This reflects a general increase in total feature usage with rising privacy concern. However, these overall trends do not indicate which specific features are more or less widely adopted in absolute terms (as shown in Figure 5a). To examine whether privacy importance is *specifically associated with the likelihood of adopting individual features*, we conducted chi-square tests of independence.

In these tests, χ^2 measures the deviation between observed and expected adoption across privacy-importance groups, while p indicates the probability that this deviation occurs by chance. The results reveal a statistically significant association only for *location protection* ($\chi^2 = 13.57$, $p = 0.009$), indicating that participants

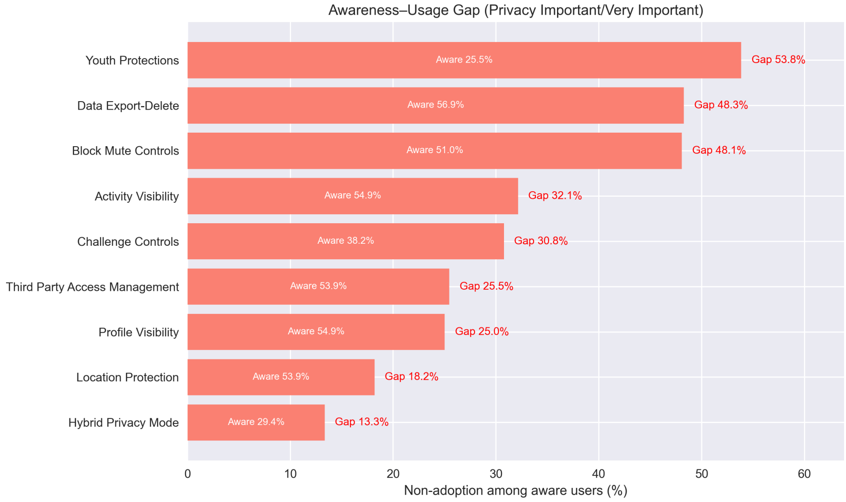


Figure 6: *Feature adoption from aware users who reported that privacy is Important/Very important to them.* The bars show the percentage of adoption for each feature, and annotations indicate the gap between awareness and actual adoption.

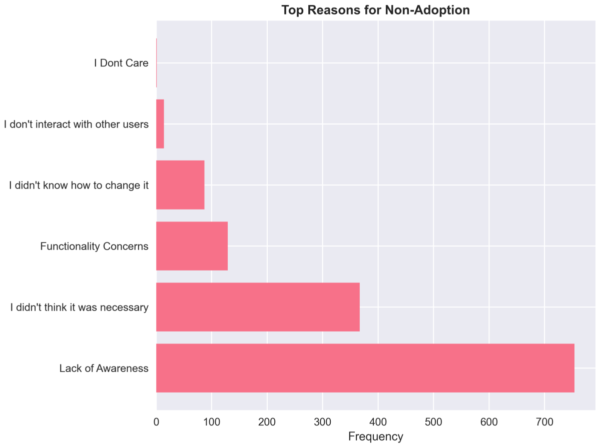


Figure 7: *Reasons for non-adoption of privacy features.* The figure illustrates the reasons reported by users for not adopting the privacy features available on fitness-tracking platforms.

who rate privacy as highly important are more likely to adopt this feature relative to those who rate privacy as less important.

Importantly, this association reflects *how strongly privacy importance predicts the likelihood of adopting a feature*, and it should not be interpreted as evidence that location protection has the highest overall adoption rate. In fact, Figure 5a shows that location protection is not the most commonly used feature. Its prominence in the chi-square analysis arises because users who rate privacy as highly important adopt location protection at a disproportionately higher rate compared to users who value privacy less, even though its absolute adoption level remains lower than that of several other features.

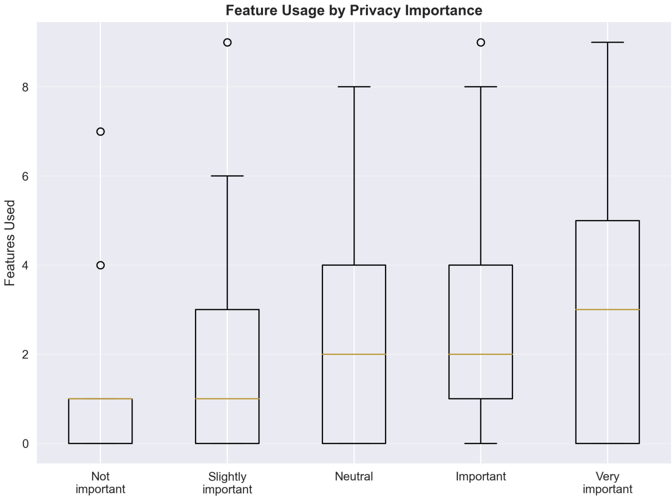


Figure 8: *Feature Adoption by Privacy Importance.* This figure shows the number of features adopted by users, grouped according to their reported level of privacy importance.

No significant associations were found for features such as *hybrid privacy mode* ($\chi^2 = 6.55$, $p = 0.162$), *block/mute controls* ($\chi^2 = 5.13$, $p = 0.274$), *challenge controls* ($\chi^2 = 3.98$, $p = 0.409$), or *profile visibility* ($\chi^2 = 3.78$, $p = 0.437$). Taken together, these findings show that while higher privacy concern corresponds to enabling more features in general, only location protection exhibits a clear statistical link between privacy importance and its adoption.

Feature Usage Correlation. Figure 10 presents the correlation matrix of privacy feature usage across participants. Correlations were calculated using Pearson's correlation coefficient, which measures the linear relationship between pairs of features, ranging from

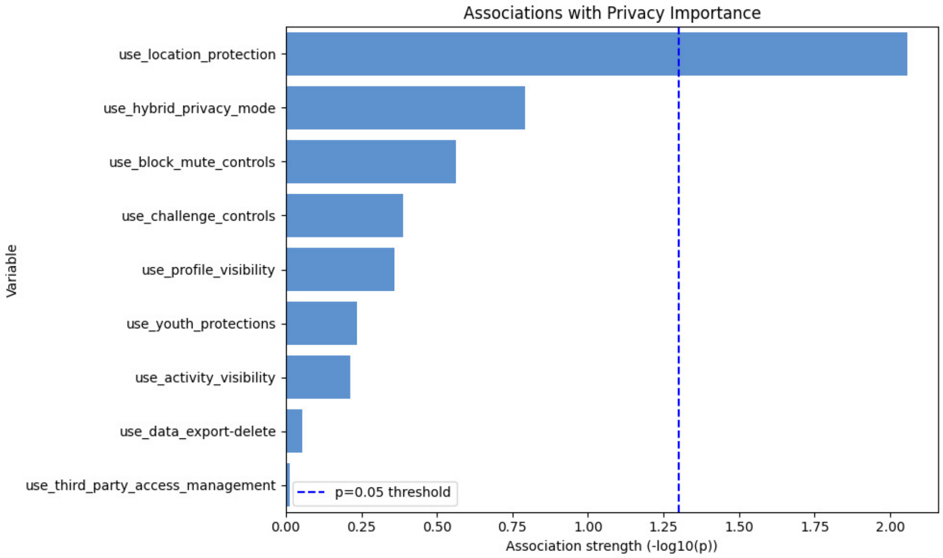


Figure 9: *Chi-Square Associations with Privacy Importance*. Bars show the strength of association between privacy importance and other variables (-log10(p-value)), with the dashed line indicating p = 0.05.

-1 (perfect negative correlation) to 1 (perfect positive correlation). The strongest positive association appears between *Profile Visibility* and *Activity Visibility* ($r = 0.75$), suggesting that users who actively manage one form of visibility tend to configure the other as well. Moderate correlations are also observed between *Hybrid Privacy Mode* and *Youth Protections* ($r = 0.50$), and between *Data Export-Deletion* and *Hybrid Privacy Mode* ($r = 0.42$). In contrast, weaker correlations (e.g., *Third Party Access Management* with most other features) indicate that certain controls are used more independently. Overall, these results highlight that while some privacy practices cluster together, others are adopted in a more isolated manner, reflecting heterogeneous strategies in user privacy management.

7.5 Latent Usage Patterns

To better understand the underlying patterns in participants' privacy feature adoption across fitness - tracking platforms, we performed dimensionality reduction and clustering on usage data.

***Principal Component Analysis and Clustering*.** To examine patterns in how users adopt privacy features on fitness platforms, we applied Principal Component Analysis (PCA) followed by k-means clustering. PCA reduces the set of correlated privacy features into independent dimensions of variation. Figure 11 plots participants along the first two principal components.

The horizontal axis (PC1) reflects *overall privacy adoption*: participants further to the right use more privacy features across the board. The vertical axis (PC2) distinguishes *types of features*, contrasting visibility controls (e.g., Profile and Activity Visibility) with protective controls (e.g., Location Protection, Data Export/Delete, Youth Protections). Red arrows show which features contribute most strongly to this separation, with longer arrows indicating stronger influence.

We then applied k-means clustering ($k = 3$) to the PCA-transformed data. Each point in the plot represents a participant, color-coded by cluster. The clusters reveal three distinct adoption profiles:

- **Cluster 0 (red, $n = 19$, avg=0.76):** High adopters who engage broadly across visibility and protective features, with Youth Protections and Location Protection especially common. Most held a Bachelor's degree.
- **Cluster 1 (blue, $n = 98$, avg=0.47):** Moderate adopters who selectively use protective controls such as Third-Party Access Management, Location Protection, and Data Export/Delete. Most reported a Master's degree.
- **Cluster 2 (green, $n = 65$, avg=0.08):** Low adopters who rarely engage with privacy features, though their limited use focused on visibility settings. Most also held a Master's degree.

In summary, Figure 11 illustrates how overall adoption (PC1) and feature type preferences (PC2) structure privacy behaviors into three meaningful user groups. In our study, we also collected demographic information on participants' education levels to explore whether education is associated with the adoption of privacy options. However, the participant pool is largely composed of Bachelor's- and Master's-level graduates, resulting in an uneven distribution across educational levels. This skew limits our ability to meaningfully examine the relationship between education and privacy adoption, and we therefore refrain from drawing conclusions about the influence of education level.

7.6 Encouragement Factors

To explore what would motivate participants to adopt more privacy features in fitness tracking platforms, we asked the open-ended question: "What would encourage you to use/adopt more privacy

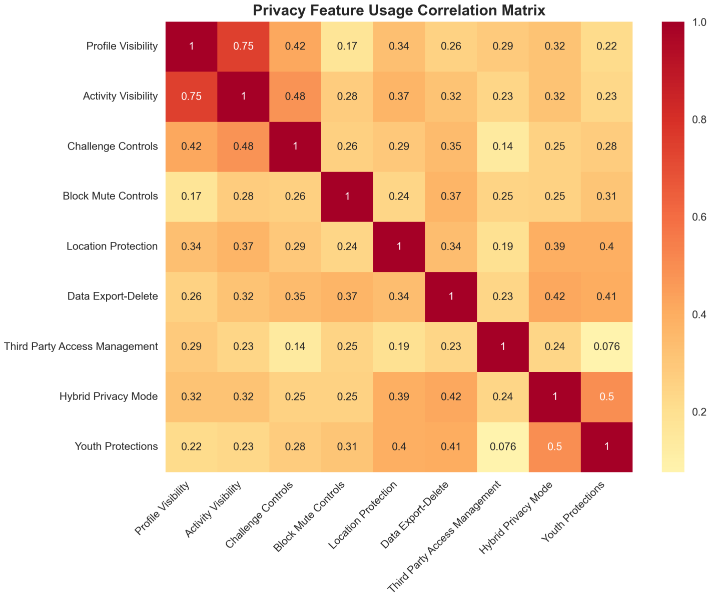


Figure 10: *Correlation matrix of privacy feature usage across participants.* Correlations were computed using Pearson’s correlation coefficient, with stronger positive values indicating features that tend to be configured together, and weaker correlations indicating more independent usage patterns.

features in fitness tracking platforms?” We analyzed responses using thematic analysis [10]. This item also functioned as a simple control question to confirm participant engagement and basic familiarity with fitness-tracking platforms. Prior to coding, we removed eight responses that contained no meaningful content, as such non-substantive answers indicate that the respondent was not attending to the survey or did not meaningfully engage with the question. The remaining valid responses were then coded into higher-level themes using a keyword-based coding scheme implemented in our analysis pipeline, producing both annotated responses and aggregate theme frequencies.

The analysis yielded seven overarching themes, which are shown in Figure 12. The most frequently cited factor was awareness and education (41 responses). Many participants emphasized that they lacked sufficient knowledge of existing controls, for instance: “More education about it and better visibility/signposting in the app” or “Knowledge on privacy features and how to use them correctly.”

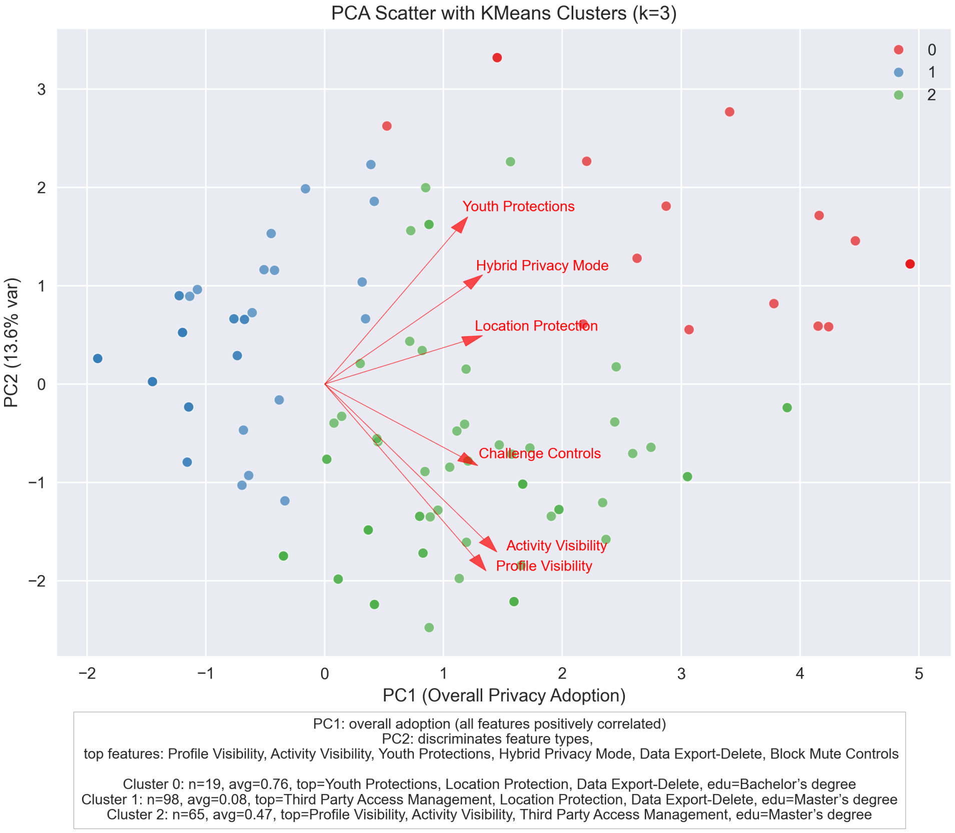
The second most prominent theme concerned risk and security concerns (36 responses). These responses were largely reactive: participants reported that they would enable or adopt privacy features in response to a perceived personal threat or evidence of data compromise (rather than proactively). Representative verbatim responses include: “If I felt there was a threat - today has taught me more about privacy features and I have turned some more on”, “If the risk of others knowing how active I am held a real danger to me. Currently it does not.”, and brief references to compromise such as “Leaks?”, “Other users’ creepy behaviour” and “rumors of privacy breach.”

Ease of use (30 responses) was another key factor. Respondents asked for simpler and more transparent settings, as illustrated by: “Easy to understand and use” and “ easy to access within the app.” Functionality concerns (25 responses) were also raised, with participants noting that they would be more likely to adopt privacy features if these did not restrict core app functionalities or competitive aspects. For instance, one respondent wrote: “If the same options/functionalities were available even with privacy.”

Trust and transparency (17 responses) highlighted the importance of platforms providing explicit and reliable information about data handling practices. Participants emphasized the need for guarantees that their personal data would be protected, alongside mechanisms to verify authenticity and integrity. Representative responses included: “I would be more encouraged to use privacy features if there were greater transparency about how my data is used.”, “Transparency about them and their impact.” and “I want transparent policies and assurance that my data is secure and only shared with my consent.”

Less frequently, participants mentioned the importance of clear communication when downloading the application (9 responses), such as straightforward explanations of privacy settings at the point of app installation: “A simple explanation video of how my data are stored, used, and sold and to give me an easy way to accept or refuse (almost like cookies on websites).” Finally, a small number of respondents expressed either uncertainty or indifference towards privacy in this context (8 responses), offering short remarks such as “Unsure” or “Not something I care about so nothing much.”

Overall, the findings suggest that adoption of privacy features depends not only on technical robustness but also on user education, transparent communication, and designs that minimize usability burdens.



PC1: overall adoption (all features positively correlated)
PC2: discriminates feature types,
top features: Profile Visibility, Activity Visibility, Youth Protections, Hybrid Privacy Mode, Data Export-Delete, Block Mute Controls

Cluster 0: n=19, avg=0.76, top=Youth Protections, Location Protection, Data Export-Delete, edu=Bachelor's degree
Cluster 1: n=98, avg=0.08, top=Third Party Access Management, Location Protection, Data Export-Delete, edu=Master's degree
Cluster 2: n=65, avg=0.47, top=Profile Visibility, Activity Visibility, Third Party Access Management, edu=Master's degree

Figure 11: *PCA plot of privacy feature adoption with KMeans clustering* ($k = 3$)*.* The figure demonstrates that PC1 captures overall adoption and PC2 distinguishes between feature types; each point represents a user, colored by cluster, and red arrows indicate the top contributing features to PC2.

8 Discussion

In this section, we interpret our findings through the lens of privacy theory and prior HCI research, and outline their implications for both design and future work.

8.1 Revisiting the Findings Through Privacy Theory

In addressing Q1 (Adoption), our empirical and survey data reveal consistently low adoption of privacy features on fitness-tracking platforms. Only 36.4% of users set their profile to private, activity-level controls are rarely used (2.12%), and Endpoint Privacy Zones (EPZs) appear in just 14.52% of analyzed activities. At the same time, one quarter of users adopt hybrid privacy configurations (25.4%), indicating a desire to balance privacy with participation in leaderboards.

These adoption patterns reflect a domain-specific manifestation of the *privacy paradox*, where users report valuing privacy yet rarely activate available protections [40, 56]. The privacy calculus framework suggests that individuals make disclosure decisions by weighing perceived benefits against potential privacy risks. Through the lens of the *privacy calculus* [18, 66, 85], users appear to view the social and motivational benefits of public visibility, such as competition, recognition, and community engagement, as outweighing abstract or uncertain privacy risks. Jamieson et al. [37] further illustrate how social norms and herding behaviors shape disclosure decisions even when individuals hold personal reservations, a dynamic that aligns closely with fitness-tracking environments.

Turning to Q2 (Reasons for Non-Adoption), our findings also resonate with research showing that privacy-control mechanisms do not always function as intended. Sannon et al. demonstrate that perceived informational control can paradoxically increase disclosure and risky behavior [64]. Our results echo this pattern: even users who are aware of privacy features often avoid enabling them because doing so reduces functionality or autonomy (for example, loss of leaderboard visibility). These functionality trade-offs highlight how traditional information-loss framings of privacy controls overlook broader user goals and platform-embedded incentives.

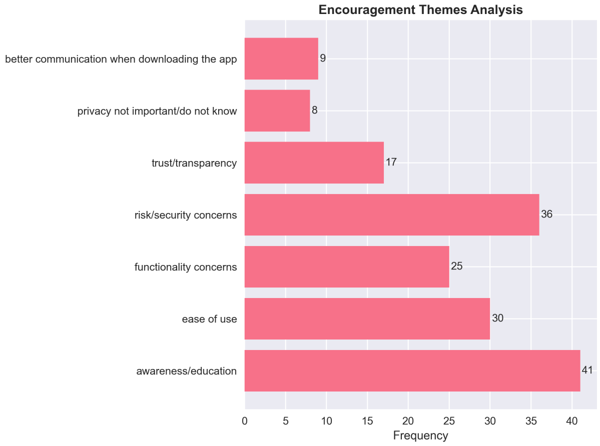


Figure 12: Themes motivating participants to adopt more privacy features in fitness tracking platforms, with the number of responses per theme.

Finally, the substantial gaps we observe between awareness and adoption point to a pronounced intention–behavior gap. Even privacy-conscious users do not consistently activate protections, often due to usability challenges, confusing settings, or low perceived necessity [9]. Together, these findings show how platform incentives, social norms, and usable-security barriers jointly shape privacy behavior in fitness-tracking contexts.

8.2 Why Awareness Does Not Translate Into Adoption

While lack of awareness was the most frequently reported barrier in our survey, awareness alone does not explain non-use. Many respondents who understood the available settings still avoided them due to functional trade-offs, low perceived necessity, or difficulty navigating menus. These findings illustrate a *usable privacy* challenge: privacy settings are fragmented, EPZ configuration is non-transparent, and defaults favor openness [14].

Social norms further discourage adoption. Much like herding effects documented in contact-tracing app use [37], appearing on leaderboards or challenges shapes expectations of visibility. Users may therefore disclose more than they intend simply to align with perceived community norms.

These findings offer several implications for privacy and HCI theory. First, they highlight contextual limitations of the privacy calculus [18, 66], as the trade-offs users face are not abstract but embedded directly in platform functionality. Consistent with Sannon et al. [64], our findings suggest that privacy models must move beyond information-loss framing to account for autonomy, motivation, and social participation.

Second, the adoption of hybrid privacy configurations reflects an emergent form of boundary regulation, where users actively combine settings to achieve intermediate states not explicitly supported by platforms, echoing the contextual nature of privacy boundary negotiation described by Palen and Dourish [59]. This mirrors observations in prior CHI work on behavioral divergence from theoretical prediction [47].

Taken together, these findings offer several lessons for the HCI community. They demonstrate that privacy behavior in fitness-tracking platforms is shaped not only by individual risk–benefit reasoning but also by the interaction design choices, defaults, and social incentives embedded in these systems, consistent with insights from usable privacy research [14]. This suggests that HCI researchers and designers should treat privacy not as a separate setting to be configured, but as an integral part of the user experience that must coexist with social, motivational, and functional goals, in line with prior work on contextual boundary negotiation [59]. More broadly, our study highlights the need for HCI theories of privacy that account for contextual incentives, boundary-regulation strategies, and the persistent intention–behavior gap, a phenomenon repeatedly documented in privacy research [9].

Finally, the observed intention–behavior gaps reinforce the need for privacy theories that incorporate friction, defaults, and interaction design as central determinants of real-world behavior.

8.3 Practical Implications: Design Recommendations

Our findings highlight several actionable directions for improving privacy engagement on fitness-tracking platforms. First, reducing configuration effort by consolidating privacy menus and simplifying navigation to core settings can help users more easily locate and adjust protections. Strengthening default safeguards, such as enabling EPZs around home or work locations or adopting followers-only profiles for new accounts, may also provide meaningful baseline protection for users who do not modify settings. Platforms could further introduce privacy-preserving competition modes that allow participation in leaderboards or challenges without revealing full identity or route details. Providing contextual cues at upload time, for example warnings about potential home-location exposure, may help users understand and respond to privacy risks in the moment. Finally, clearer explanations of privacy–functionality trade-offs can help users make informed choices about which protections to enable without undermining their engagement with social and motivational features.

9 Conclusions

This is the first large-scale study to provide a structured overview of privacy features across fitness-tracking platforms, highlighting key similarities and differences. Our analysis of Strava and Garmin Connect reveals a significant gap between the availability of privacy controls and their actual use. A user study with 182 participants further explores the reasons for this underutilization and identifies factors that could encourage users to adopt these features.

Acknowledgments

We thank the anonymous reviewers for their constructive feedback. The research conducted in this paper was triggered by the project "Collaborative, Multi-modal and Agile Professional Cybersecurity Training Program for a Skilled Workforce In the European Digital Single Market and Industries" (CyberSecPro) project. This project has received funding from the European Union's Digital Europe Programme (DEP) programme under grant agreement No 101083594. The authors are grateful for the financial support of this project that has received funding from the European Commission. The views expressed in this paper represent only the views of the authors and not of the European Commission or the partners in the above-mentioned project. This work was also supported by the European Union's Horizon 2020 programme under Grant Agreement No. 101070599 (SecOPERA).

References

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2020. Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology* 30, 4 (2020), 736–758.

[2] Alessandro Acquisti and Ralph Gross. 2006. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *International workshop on privacy enhancing technologies*. Springer, 36–58.

[3] Angeliki Aktypi, Jason RC Nurse, and Michael Goldsmith. 2017. Unwinding Ariadne's identity thread: Privacy risks with fitness trackers and online social networks. In *Proceedings of the 2017 on Multimedia Privacy and Security*. 1–11.

[4] Majed Almansoori and Rahul Chatterjee. 2025. Can Social Media Privacy and Safety Features Protect Targets of Interpersonal Attacks? A Systematic Analysis. *Proceedings on Privacy Enhancing Technologies* (2025).

[5] Under Armour. 2024. MapMyRun Privacy Policy. https://www.mapmyrun.com/privacy/. Accessed: 2025-01-07.

[6] Under Armour. 2024. Privacy Settings in MapMyRun. https://www.mapmyrun.com/help/. Accessed: 2025-01-07.

[7] ASICS. 2024. Privacy Settings in Runkeeper. https://runkeeper.com/help/privacy. Accessed: 2025-01-07.

[8] ASICS. 2024. Runkeeper Privacy Policy. https://runkeeper.com/privacy. Accessed: 2025-01-07.

[9] Lemi Baruh, Ekin Secinti, and Zeynep Cemalcilar. 2017. Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication* 67, 1 (2017), 26–53.

[10] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[11] Ji Yeon Cho, Daesun Ko, and Bong Gyou Lee. 2018. Strategic Approach to Privacy Calculus of Wearable Device User Regarding Information Disclosure and Continuance Intention. *KSII Transactions on Internet & Information Systems* 12, 7 (2018).

[12] Jacob Cohen. 1992. Statistical power analysis. *Current directions in psychological science* 1, 3 (1992), 98–101.

[13] Garmin Connect. 2024. Garmin Connect - Free Online Fitness Community. "https://connect.garmin.com/"

[14] Lorrie F Cranor. 2008. A framework for reasoning about the human in the loop. (2008).

[15] Roba Darwish and Kambiz Ghazinour. 2019. Photos and Tags: A Method to Evaluate Privacy Behavior. In *Intelligent Computing: Proceedings of the 2019 Computing Conference, Volume 2*. Springer, 797–816.

[16] Yves-Alexandre De Montjoye, César A Hidalgo, Michel Verleysen, and Vincent D Blondel. 2013. Unique in the crowd: The privacy bounds of human mobility. *Scientific reports* 3, 1 (2013), 1376.

[17] Karel Dhondt, Victor Le Pochat, Alexios Voulimeneas, Wouter Joosen, and Stijn Volckaert. 2022. A Run a Day Won't Keep the Hacker Away: Inference Attacks on Endpoint Privacy Zones in Fitness Tracking Social Networks. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*, Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi (Eds.). ACM, 801–814. doi:10.1145/3548606.3560616

[18] Tamara Dinev and Paul Hart. 2006. Internet privacy concerns and their antecedents—measurement validity and a regression model. *Behaviour & Information Technology* 25, 6 (2006), 413–422.

[19] EPZ 2024. Edit map visibility – Strava support. https://support.strava.com/hc/en-us/articles/115000173384-Edit-Map-Visibility

[20] Facebook. 2024. Facebook. https://www.facebook.com Accessed: 2024-02-20.

[21] Fitbit. 2024. Fitbit Data Privacy Settings. https://www.fitbit.com/global/privacy/. Accessed: 2025-01-07.

[22] Fitbit. 2024. Fitbit Privacy Policy. https://www.fitbit.com/privacy/policy. Accessed: 2025-01-07.

[23] Rob Franken, Hidde Bekhuis, and Jochem Tolsma. 2023. Kudos make you run! How runners influence each other on the online social network Strava. *Social Networks* 72 (2023), 151–164.

[24] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users' expectations about and use of smartphone privacy and security settings. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–24.

[25] Thomas Fritz, Elaine M Huang, Gail C Murphy, and Thomas Zimmermann. 2014. Persuasive technology in the real world: a study of long-term use of activity sensing devices for fitness. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 487–496.

[26] Sandra Gabriele and Sonia Chiasson. 2020. Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–12.

[27] Garmin. 2024. Garmin Connect Privacy Guide. https://www.garmin.com/en-US/legal/privacy-policy/. Accessed: 2025-01-07.

[28] Garmin. 2024. Privacy Settings for Garmin Connect. https://www.garmin.com/en-US/legal/privacy-policy/. Accessed: 2025-01-07.

[29] Philippe Golle and Kurt Partridge. 2009. On the anonymity of home/work location pairs. In *International Conference on Pervasive Computing*. Springer, 390–397.

[30] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs. 2018. The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–14.

[31] Ralph Gross and Alessandro Acquisti. 2005. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. 71–80.

[32] John A Hartigan and Manchek A Wong. 1979. Algorithm AS 136: A k-means clustering algorithm. *Journal of the royal statistical society. series c (applied statistics)* 28, 1 (1979), 100–108.

[33] Wajih Ul Hassan, Saad Hussain, and Adam Bates. 2018. Analysis of privacy protections in fitness tracking social networks-or-you can run, but can you hide?. In *27th USENIX Security Symposium (USENIX Security 18)*. 497–512.

[34] Luca Hernández Acosta, Sebastian Rahe, and Delphine Reinhardt. 2022. Does Cycling Reveal Insights About You? Investigation of User and Environmental Characteristics During Cycling. In *International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services*. Springer, 172–190.

[35] Sharon Heung, Lucy Jiang, Shiri Azenkot, and Aditya Vashistha. 2024. "Vulnerable, Victimized, and Objectified": Understanding Ableist Hate and Harassment Experienced by Disabled Content Creators on Social Media. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–19.

[36] David W Hosmer Jr, Stanley Lemeshow, and Rodney X Sturdivant. 2013. *Applied logistic regression*. John Wiley & Sons.

[37] Jack Jamieson, Daniel A Epstein, Yunan Chen, and Naomi Yamashita. 2022. Unpacking intention and behavior: Explaining contact tracing app adoption and hesitancy in the United States. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–14.

[38] Hongbo Jiang, Jie Li, Ping Zhao, Fanzi Zeng, Zhu Xiao, and Arun Iyengar. 2021. Location privacy-preserving mechanisms in location-based services: A comprehensive survey. *ACM Computing Surveys (CSUR)* 54, 1 (2021), 1–36.

[39] Ian T Jolliffe and Jorge Cadima. 2016. Principal component analysis: a review and recent developments. *Philosophical transactions of the royal society A: Mathematical, Physical and Engineering Sciences* 374, 2065 (2016), 20150202.

[40] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security* 64 (2017), 122–134.

[41] Balachander Krishnamurthy and Craig E Wills. 2008. Characterizing privacy in online social networks. In *Proceedings of the first workshop on Online social networks*. 37–42.

[42] John Krumm. 2007. Inference attacks on location tracks. In *International Conference on Pervasive Computing*. Springer, 127–143.

[43] Hao-Ping Lee, Yu-Ju Yang, Thomas Serban Von Davier, Jodi Forlizzi, and Sauvik Das. 2024. Deepfakes, phrenology, surveillance, and more! a taxonomy of ai privacy risks. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–19.

[44] Debora Benedetta Lombardi and Maria Rita Ciceri. 2016. More than defense in daily experience of privacy: The functions of privacy in digital and physical environments. *Europe's journal of psychology* 12, 1 (2016), 115.

[45] Garmin Ltd. 2024. 2024 Annual Report. https://www8.garmin.com/aboutGarmin/invRelations/reports/2024_Annual_Report.pdf Accessed: 2025-08-17.

[46] Garmin Ltd. 2024. 2024 Corporate Impact Report. https://www8.garmin.com/sustainability/reports-policies/corp-responsibility/Corporate_Impact_Report_2024.pdf Accessed: 2025-08-17.

[47] Dominique Machuletz, Stefan Laube, and Rainer Böhme. 2018. Webcam covering as planned behavior. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.

[48] MapMyRun 2024. MapMyRun. https://www.mapmyrun.com/

[49] Mary L McHugh. 2013. The chi-square test of independence. *Biochemia medica* 23, 2 (2013), 143–149.

[50] Ülkü Meteriz, Necip Faziotal Yiotaldiotaran, Joongheon Kim, and David Mohaisen. 2020. Understanding the Potential Risks of Sharing Elevation Information on Fitness Applications. In *40th IEEE International Conference on Distributed Computing Systems, ICDCS 2020, Singapore, November 29 - December 1, 2020*. IEEE, 464–473. doi:10.1109/ICDCS47774.2020.00063

[51] Ulku Meteriz-Yildiran, Necip Fazil Yildiran, Joongheon Kim, and David Mohaisen. 2022. Learning Location from Shared Elevation Profiles in Fitness Apps: A Privacy Perspective. *IEEE Transactions on Mobile Computing* (2022).

[52] Michael Methlagl, Friederike Michlmayr, and Valentina Perillo. 2023. Technological trust perceptions in wearable fitness technology: a person-centred approach. *Journal of Technology in Behavioral Science* 8, 4 (2023), 392–401.

[53] Preksha Nema, Pauline Anthonysamy, Nina Taft, and Sai Teja Peddinti. 2022. Analyzing user perspectives on mobile app privacy at scale. In *Proceedings of the 44th international conference on software engineering*. 112–124.

[54] Nike. 2024. Nike Run Club Privacy Policy. https://www.nike.com/privacy-policy. Accessed: 2025-01-07.

[55] Nike. 2024. Privacy Settings in Nike Run Club. https://www.nike.com/help/. Accessed: 2025-01-07.

[56] Patricia A Norberg, Daniel R Horne, and David A Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs* 41, 1 (2007), 100–126.

[57] Business of Apps. 2025. Fitbit Statistics 2025: Revenue, Devices Sold, Users, and Usage. https://www.businessofapps.com/data/fitbit-statistics/

[58] Business of Apps. 2025. Strava Revenue and Usage Statistics (2025). https://www.businessofapps.com/data/strava-statistics/

[59] Leysia Palen and Paul Dourish. 2003. Unpacking" privacy" for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 129–136.

[60] Peter Peduzzi, John Concato, Elizabeth Kemper, Theodore R Holford, and Alvan R Feinstein. 1996. A simulation study of the number of events per variable in logistic regression analysis. *Journal of clinical epidemiology* 49, 12 (1996), 1373–1379.

[61] PRAW Developers. 2025. *PRAW: The Python Reddit API Wrapper.* https://praw.readthedocs.io/en/stable/ Accessed: 2025-02-25.

[62] Elissa M. Redmiles, Yasemin Acar, Sascha Fahl, and Michelle L. Mazurek. 2017. *A Summary of Survey Methodology Best Practices for Security and Privacy Researchers.* Technical Report CS-TR-5055. University of Maryland, College Park.

[63] Kavous Salehzadeh Niksirat, Lev Velykoivanenko, Noé Zufferey, Mauro Cherubini, Kévin Huguenin, and Mathias Humbert. 2024. Wearable activity trackers: A survey on utility, privacy, and security. *Comput. Surveys* 56, 7 (2024), 1–40.

[64] Shruti Sannon, Natalya N Bazarova, and Dan Cosley. 2018. Privacy lies: Understanding how, when, and why people lie to protect their privacy in multiple online contexts. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–13.

[65] Selenium 2024. Selenium WebDriver. https://www.selenium.dev/documentation/webdriver/

[66] H Jeff Smith, Tamara Dinev, and Heng Xu. 2011. Information privacy research: an interdisciplinary review. *MIS quarterly* (2011), 989–1015.

[67] Strava. 2023. Strava Year In Sport Trend Report: Insights on the World of Exercise. https://stories.strava.com/articles/strava-year-in-sport-trend-report-insights-on-the-world-of-exercise

[68] Strava. 2024. Privacy Settings. https://www.strava.com/settings/privacy. Accessed: 2025-01-07.

[69] Strava 2024. Strava - Running, Cycling & Hiking App - Train, track & share. https://www.strava.com/

[70] Strava. 2024. Strava Privacy Policy. https://www.strava.com/legal/privacy. Accessed: 2025-01-07.

[71] Strava. 2025. Strava Reaches Over 150 Million Registered Users Globally. *Wall Street Journal* (2025). https://www.wsj.com/tech/personal-tech/strava-athlete-intelligence-michael-martin-ceo-37c9a993 Accessed: 2025-08-17.

[72] Strava Support. 2025. *Create a Segment.* https://support.strava.com/hc/en-us/articles/216918157-Create-a-Segment

[73] Strava Support. 2025. Edit Map Visibility. https://support.strava.com/hc/en-us/articles/115000173384-Edit-Map-Visibility Accessed: 2025-02-17.

[74] Bartlomiej Surma, Tahleen Rahman, Monique Breteler, Michael Backes, and Yang Zhang. 2023. You Are How You Walk: Quantifying Privacy Risks in Step Count Data. *arXiv preprint arXiv:2308.04933* (2023).

[75] SurveyCircle. 2025. Research website SurveyCircle. https://www.surveycircle.com

[76] SurveySwap. 2025. SurveySwap: Find Survey Participants Today. https://surveyswap.io

[77] Mohammad Tahaei, Tianshi Li, and Kami Vaniea. 2022. Understanding privacy-related advice on stack overflow. *Proceedings on Privacy Enhancing Technologies* (2022).

[78] Mohammad Tahaei, Kami Vaniea, and Naomi Saphra. 2020. Understanding privacy-related questions on stack overflow. In *Proceedings of the 2020 CHI conference on human factors in computing systems*. 1–14.

[79] Joshua Tan, Khanh Nguyen, Michael Theodorides, Heidi Negrón-Arroyo, Christopher Thompson, Serge Egelman, and David Wagner. 2014. The effect of developer-specified explanations for permission requests on smartphone user behavior. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 91–100.

[80] Sabine Theis, Carolin Stellmacher, Sebastian Pütz, Matthias G Arend, and Verena Nitsch. 2023. Understanding fitness tracker users' and non-users' requirements for interactive and transparent privacy information. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–7.

[81] Lev Velykoivanenko, Kavous Salehzadeh Niksirat, Noé Zufferey, Mathias Humbert, Kévin Huguenin, and Mauro Cherubini. 2021. Are those steps worth your privacy? Fitness-tracker users' perceptions of privacy and utility. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 4 (2021), 1–41.

[82] Jessica Vitak, Yuting Liao, Priya Kumar, Michael Zimmer, and Katherine Kritikos. 2018. Privacy attitudes and data valuation among fitness tracker users. In *International Conference on Information*. Springer, 229–239.

[83] Eric Vittinghoff and Charles E McCulloch. 2007. Relaxing the rule of ten events per variable in logistic and Cox regression. *American journal of epidemiology* 165, 6 (2007), 710–718.

[84] X. 2024. X (formerly Twitter). https://x.com Accessed: 2024-02-20.

[85] Heng Xu, Hock-Hai Teo, and Bernard Tan. 2005. Predicting the adoption of location-based services: the role of trust and perceived privacy risk. (2005).

[86] Wei Zhou and Selwyn Piramuthu. 2014. Security/privacy of wearable fitness tracking IoT devices. In *2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE, 1–5.

[87] Noé Zufferey, Mathias Humbert, Romain Tavenard, and Kévin Huguenin. 2023. Watch your watch: inferring personality traits from wearable activity trackers. In *32nd USENIX Security Symposium (USENIX Security 23)*. 193–210.

[88] Noé Zufferey, Kavous Salehzadeh Niksirat, Mathias Humbert, and Kévin Huguenin. 2023. "Revoked just now!" Users' Behaviors Toward Fitness-Data Sharing with Third-Party Applications. *Proc. Priv. Enhancing Technol.* 2023, 1 (2023), 47–67.

A Logistic Regression Analysis of Privacy Feature Adoption

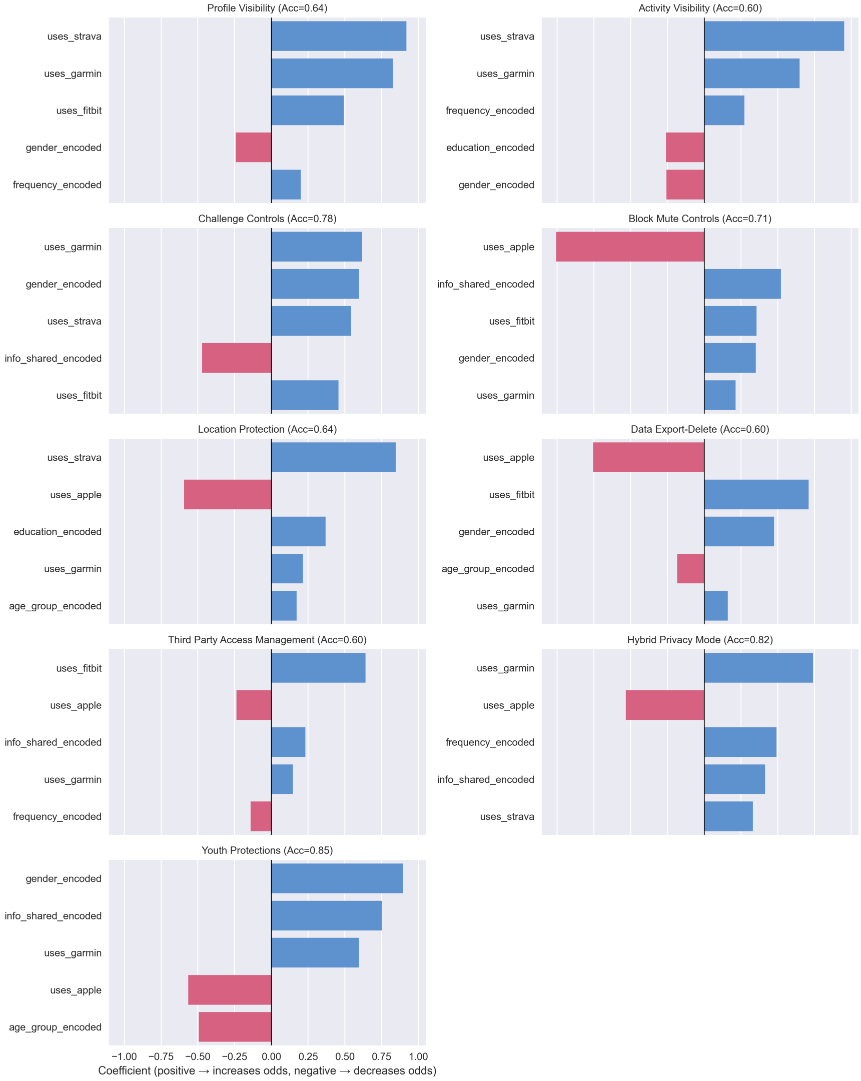


Figure 13: *Logistic Regression Analysis of Privacy Feature Adoption.* The figure presents the top predictors for adoption of each privacy feature based on logistic regression models. Bars represent regression coefficients, with positive values (blue) indicating predictors that increase the odds of adoption and negative values (red) indicating predictors that decrease the odds. Model accuracies are reported for each feature, and only the top predictors by absolute coefficient magnitude are shown for clarity.