Exploring The Design Space of Sharing and Privacy Mechanisms in Wearable Fitness Platforms

Abdulmajeed Alqhatani
University of North Carolina at Charlotte
aalqhata@uncc.edu

Heather R. Lipford
University of North Carolina at Charlotte
Heather.Lipford@uncc.edu

***Abstract*—Users of wearable fitness devices share different pieces of information with a variety of recipients to support their health and fitness goals. Device platforms could ease this sharing and empower users to protect their information by providing controls and features centered around these common sharing goals. However, there is little research that examines existing mechanisms for sharing and privacy management, and what needs users have beyond their current controls. In this paper, we analyze five popular wearable device platforms to develop taxonomies of mechanisms based on common sharing patterns and boundaries, as well as data collection awareness. With this analysis, we identify design opportunities for supporting users' sharing and privacy needs.**

I. Introduction

Over the last few years, wearable fitness devices have become very popular. Reports estimate that 520.1 million units of commercial wearable devices will be sold in 2025, which are almost triple the number of units that were sold in the previous year [4]. Users of these devices can enjoy tracking a variety of health and fitness data, such as step count, distance, sleep pattern, calories consumed, vital signs, and others. Wearable fitness devices are part of the so-called "quantified self"— monitoring and analyzing aspects of one's body and life using digital technologies [13].

Popular devices, such as Fitbit, have companion apps that enable users to gain deeper insights about their tracked data. Many of these apps also have features to share self-tracking data with different entities. Social sharing can provide positive effects on users' activity levels [8]. Users can be motivated to exercise and exchange health and fitness knowledge within online communities. Thus, sharing self-tracking data has become a common practice by users of these devices. Users may also connect their device app to several compatible apps to take advantage of additional features, such as tracking exercises with maps.

However, collecting information pertaining to health and fitness and sharing it raises privacy concerns, such as inferences, repurposing, and stalking. Data collected by these devices can be used to infer private aspects about users [19]. If wearable device data is combined with other information (e.g., social media and public profiles), it may even reveal a person's real identity [1]. Users are widely concerned that organizational actors, such as markets and insurers may utilize such data in a harmful way, such as product and insurance discrimination. Privacy risks can extend to the social level when users share their data with other individuals. For example, movement and location data can be used by stalkers and criminals to learn about users' daily routines.

Fortunately, users can prevent or mitigate these risks through various platform controls— mainly privacy settings. These controls should be complemented with some awareness mechanisms that help users understand the potential risks of providing their data to different collectors. Yet, little is known about how current platforms support users in managing their privacy, and what mechanisms these platforms have in common. This paper explores wearable fitness device platforms regarding sharing and privacy control mechanisms. It compares and classifies popular platforms based on their sharing patterns and data collection awareness mechanisms. This study has the following two research questions:

1) What controls and mechanisms do current wearable device platforms have for sharing and privacy management?
2) What new mechanisms are needed to better match users' desired sharing practices and privacy needs?

The main goal is to identify unexplored design opportunities around these mechanisms, which can serve as a roadmap for future research interested in building solutions for managing personal privacy in fitness trackers.

II. Background

In this section, we provide an overview about wearable fitness devices and discuss the privacy issues related to this technology. We then review previous research on sharing and privacy mechanisms.

A. Wearable Fitness Trackers and Privacy

A variety of commercial wearable devices for tracking health and fitness are now widely used. We define these devices as any devices with embedded sensors, and typically internet connection capability, that can be worn on the body to collect various health and fitness data. These devices

Workshop on Usable Security and Privacy (USEC) 2021
7 May 2021, Auckland, New Zealand
ISBN 1-891562-73-8
https://dx.doi.org/10.14722/usec.2021.23009
www.ndss-symposium.org

commonly have their own platform that enables users to analyze their self-tracking data. Fitbit is one popular example of commercial fitness wearables, which enable users to track daily and weekly movement data, calories consumed, sleep pattern and several other metrics.

Many of these platforms also have embedded social communities to interact with other users, as well as features to integrate with different external platforms, such as social media applications. Sharing with others provides motivation and accountability, and enhances interpersonal relationships [8]. Thus, sharing fitness information through these platforms have become an important part of many users' practices toward achieving their health and fitness goals [5, 10]. For example, one study found that half of their participants utilized the sharing features within their device platform to support their fitness activities [7].

Users have different preferences regarding what information to share and with whom. For example, we conducted an interview study with wearable fitness tracker users and found that participants shared their fitness information with six groups of recipients, namely friends, family, strangers, physicians, incentive programs and co-workers, each associated with particular health and fitness goals [2]. Another study showed that fitness tracker users were less willing to share their demographic information than health information collected by a device; more willing to share information with strangers than family members and friends; and more willing to share information with specific third parties than the general public [18]. All these different sharing preferences suggest that users can be concerned about the privacy of their fitness information.

Sharing data collected by wearable fitness devices also imposes several privacy concerns. There is a wide concern that companies, including a device manufacturer itself, might utilize consumers' data without their awareness for secondary purposes. Data is typically stored anonymously in the manufacturers' databases, but they are still prone to inferences and even re-identification if the fitness tracker data is correlated with data from other sources [1, 24]. Studies have demonstrated that highly private information can be derived from the different sensors available in these devices [11].

Therefore, a device platform should provide mechanisms that empower users to control the sharing of their information and make them aware of what other personal information could be collected about them.

B. Sharing and Privacy Mechanisms

Fitness device users can utilize different platform mechanisms to control access into their information by other users and organizational actors. These mechanisms should be flexible in order to meet users' varying levels of privacy preferences (what, how, when, and with whom). Yet, we lack a study that collectively examines multiple platforms regarding their mechanisms for privacy management, and what new mechanisms are needed to better match users' preferences.

Those few studies that examined the platforms of commercial Internet of Things (IoT) devices aimed to gain insights into their structure, and design similarities and differences. For example, Mare et al. [14] examined several smart home systems to explore their design choices with respect to access control, privacy, and automation. In terms of fitness trackers, Witte et al. [23] analyzed and categorized ten popular wearable device platforms to understand their ecosystem as a whole. They found similar mechanisms among these platforms, such as the features to integrate with social media applications. Other research focused on managing the complexity of data access and sharing settings in IoT platforms by recommending privacy settings that can match users' preferences [3, 22]. For example, the work by Torre et al. [22] implemented a data-driven approach to design a set of customizable privacy settings recommendations in fitness trackers.

In our study, we explore the design opportunities based on sharing patterns and data collection awareness mechanisms. We believe that these mechanisms are important because they deal with how people can manage their privacy when disclosing personal data with different entities, including individuals, device manufacturers, and third parties.

III. DESIGN SPACE EXPLORATION

The purpose of this paper is to explore the design space of sharing and privacy mechanisms in the context of wearable fitness technology. Our study provides a broader view by examining five wearable device platforms that are used for tracking personal activity. These devices also have mobile apps with several sharing features. Our chosen platforms are: Fitbit, Apple Watch Activity, Polar Flow, Garmin Connect, and Samsung Health. These brands are among the top selling brands on the wearable market in the last few years [21]. We analyzed all platforms in May and June 2020. The first author purchased the devices in order to access their functionalities and to understand their privacy controls and sharing mechanisms. We specifically investigated these platforms regarding two main themes: sharing patterns and data collection awareness mechanisms.

We first systematically examined all the sharing and privacy features within a particular device, and made note of all features and screens we were able to. We then organized the features to create a taxonomy of their mechanisms. In particular, we wanted to understand what features a platform has for supporting all possible sharing patterns, inside or outside a platform. In a previous study, we identified a comprehensive set of sharing patterns by users [2], and thus we used these patterns as a basis for analyzing the five platforms. Second, systems commonly make users aware of their own privacy through different means. We are interested in how a device platform may communicate privacy aspects during their regular interaction with a system. This includes information requested from users in the account creation and any interface notifications or nudges related to privacy. The usability of privacy policies and Terms of Service (ToS) Agreements is a challenge that has been extensively addressed. Thus, we considered this aspect outside the scope of this analysis. Our current work identifies commonalities and differences in controls and features available within wearable fitness devices and presents a set of taxonomies.

IV. FINDINGS

We first examine sharing mechanisms in these platforms based on several sharing patterns. Sharing fitness tracker data can generally occur in two ways: inside a platform with other users and communities (e.g. Fitbit communities), or on external compatible third-party apps (e.g. social media apps). Users can utilize various controls to manage internal sharing, and have general controls to manage sharing self-tracking data with third parties. We will discuss features and controls for both sharing methods in more detail. In the second part of this section, we briefly describe platform mechanisms for data collection awareness.

A. Sharing Mechanisms

Sharing decisions of fitness tracker users are goal-driven with audiences and specific practices related to those goals; for instance, a common practice by users who share with friends is to utilize popular social media channels, such as Facebook and Twitter [2]. Thus, we focus on investigating whether platforms support these patterns and what mechanisms they have in common for each of these patterns.

Friends Pattern. All the examined platforms have social features that enable users to form a connection (e.g., friendship) with other individuals in these platforms. Typically, sharing with other people over these platforms requires that both sides have a device from the same manufacturer. To connect with another user, Apple Activity and Samsung Health users needs the other user's ID, such as the email or phone number that is linked to the account.

Given that these platforms have sharing features similar to those in common social network sites, we looked at their boundary mechanisms to categorize and further discuss the controls people can utilize when interacting with friends over these platforms (Table 2). Boundary mechanisms are interface controls that can be used to restrict other users' access to oneself. These controls have been extensively studied in social media platforms [9, 12], but not yet in the context of IoT device platforms.

The first boundary, relationship, refers to controlling who can be part of a personal social network. Regardless of the type of relationship, all the examined platforms except Fitbit, which has a family feature, have the same settings for all connections including friends. There are two types of controls for managing connection boundaries that are similar in these platforms: accept/decline connection requests and remove/stop following friends. All platforms support these two options except for Samsung Health. There, any user can be followed by others if they know the intended user's account ID.

The territorial boundary is the regulation of who can view an individual's "personal space", in this case, their personal profile information, including their friends list. All platforms allow users to stay private, or to share information with friends/followers. Garmin Connect provides more privacy options than the other platforms— it also offers users to keep their data private or to share it with followers, groups & followers, or public. Apple Watch activity is the only one that allows users to hide information from particular friends.

There are several levels to control the visibility of information within a profile (e.g., leaderboard, activity, training, and challenges), and these levels vary between the examined platforms (Table 3). For example, Fitbit has controls for each piece of profile information, while Apple Activity settings are less flexible than the other platforms in that the entire profile will be hidden. Note that profile information in the Apple Activity differs from the other platforms in that it includes activity information only, rather than additional personal information, such as age and gender. Polar Flow and Garmin Connect links the visibility of friend list to the entire profile visibility.

The disclosure boundary deals with controlling the disclosure of one's own personal information. Currently, there are three main categories of personal information that users can disclose to other people over these platforms. First, the profile information which mostly includes gender, age, birthdate, weight, and height. We discussed the controls related to profile information in the territorial boundary. The second category of information that users will be able to disclose is the daily activity summary. The level of granularity differs depending on a platform. Users will mostly be able to share daily step count, distance, active minutes, and calories burned. Depending on the privacy settings selected by a user, Apple Watch Activity, Polar Flow, Garmin Connect, and Samsung Health automatically share a daily activity summary with friends. For Fitbit users, they need to push summary of their data to other users. The third category is exercise sessions, such as walking,

TABLE I: Taxonomy of the Sharing Pattern Mechanisms in Five Wearable Device Platforms.

Pattern	Sharing Mechanism	Fitbit	Apple Activity	Polar Flow	Garmin Connect	Samsung Health
Friends	Screenshot of activity	✓	✓	X	X	✓
	Photo with summary	X	X	✓	✓	✓
	Web link	X	X	X	✓	X
Family	Family account feature	✓	X	X	X	X
Strangers	Fitness group feature	✓	X	✓	✓	X
	External fitness community	✓	X	✓	✓	X
Caregivers	N/A					
Incentive Programs	Rewards through 3rd party app	✓	X	✓	X	X
Workplace	Corporate Wellness Program	✓	X	✓	✓	X
	Built-in fitness groups	✓	X	✓	✓	X

running, and cycling. Most devices will automatically detect this data using their various sensors, otherwise users need to log their workouts manually. This data requires an action by a user by pushing it to other people, except in Polar Flow, which will automatically upload data to connections based on the user's selected settings.

If users need further restrictions in terms of others' access to oneself, then they may utilize the interactional boundary controls. There are four areas where these types of controls can be used: disabling friendship requests, disabling comments, disabling likes/cheering, and blocking users. Except for Fitbit and Samsung Health, all users will be able to withdraw a friendship request that they sent to other users. One cannot post comments to other Samsung users, and comments to Apple Watch users will be sent in the form of text messages. In addition, both Apple Watch Activity and Samsung Health do not offer features for liking or cheering. Fitbit and Polar Flow users can remove likes, but they cannot remove posted comments. Sometimes users need to prevent other users from finding their profiles or sending them friendship requests, and thus they may take advantage of the block user feature. Currently, Fitbit, Polar Flow, and Garmin Connect users can block other individuals through the intended individual profile pages. Samsung Health allows one to hide his/her ID from being searched by other users but does not offer the block feature. Activity is the fitness tracking app for Apple Watch, but some of its data needs to be managed through the phone settings. Users can add their connections on the Activity app as contacts in the phone, and thus they will be able to block messages from them. However, other users will still be able to send someone a friendship request if they have his/her account ID. Only Garmin connect provides users controls to manage all forms of interaction with other people.

In our previous study, we found that users who share their activity data with friends commonly use social media sites outside of the device platform, but users faced concerns over the broad audience on those platforms [2]. Thus, the most important design aspect in the context of this pattern is whether a platform supports sharing data on social media applications and how. All the five platforms allow their users to share self-tracking data on the social media applications installed in the user's mobile phone by pushing a summary of data to these applications. Fitbit, Apple Activity, and Samsung Health allow users to push charts with a summary of data shown on them. Polar Flow, Garmin Connect, and Samsung Health users can also choose an existing photo in the phone or take a new one and share it. Depending on an exercise type, Polar Flow allows sharing a map of exercise routes with a summary of data shown on it. Garmin Connect users can also share a web link that will take recipients to a Garmin page that has a variety of data about the exercise.

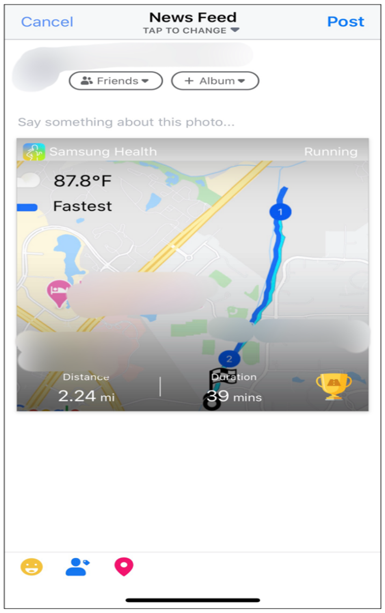


Fig. 1: Sharing Data from Fitness Tracker to Facebook (Samsung Health).

The level of data that can be shared on social media applications varies, depending on what can be collected by a device. For example, Samsung Health enables sharing a variety of granular data, such as movement data (e.g., step count, duration, and intervals), heart rate (e.g., average and resting heart rate) and calories consumed (e.g., carbs, fat, and protein). Apple Activity enables recording several exercises and data, but it visualizes three abstract rings that represent the level of "move," "exercise," and "stand" when data is shared externally with other people.

In terms of audiences, if users need to share their fitness data on social media applications and specify particular audiences, they can adjust that from the settings of the destination platform only (e.g., Fig. 1). Facebook, for example, offers different categories of connection (e.g., acquaintances, friends, close friends).

TABLE II: Taxonomy of Boundary Controls in Wearable Fitness Platforms.

Boundary	Controls	Fitbit	Apple Activity	Polar Flow	Garmin Connect	Samsung Health
Relationship	Accept/decline friendship	✓	✓	✓	✓	X
	Remove friend/stop following	✓	✓	✓	✓	✓
Territorial	Profile visibility	✓	X	✓	✓	✓
Disclosure	Customizating information	✓	✓	✓	✓	✓
Interactional	Disable friendship	X	✓	✓	✓	X
	Disable comments	X	✓	X	✓	N/A
	Disable likes/cheers	✓	N/A	✓	✓	N/A
	Block users	✓	X	X	✓	✓

TABLE III: Visibility Controls of Activity Information.

Level	Fitbit	Apple Activity	Polar Flow	G. Connect	S. Health
Private	✓	✓	✓	✓	✓
Followers	✓	✓	✓	✓	✓
Customized	X	✓	X	X	X
My Groups & Followers	X	X	X	✓	X
Public	✓	✓	✓	✓	✓

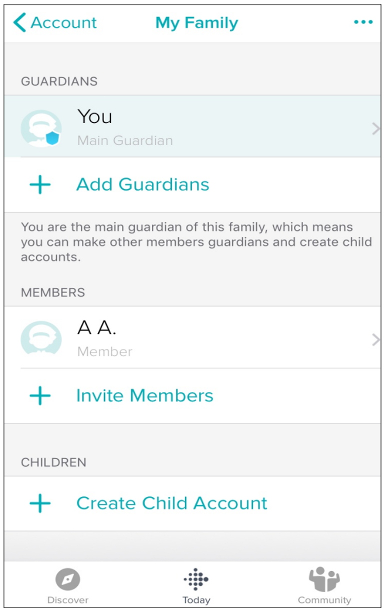
In summary, all the five platforms enable sharing activity data with friends within a platform and on social media sites. However, the level of granularity depends on the controls offered by a platform. The interpersonal boundary controls in these platforms include relationship, territorial, disclosure, and interaction. Overall, Garmin Connect is the best platform in supporting the identified interpersonal boundary controls, and Samsung Health provides the least support of these controls.

Family Pattern. Users seek mutual accountability and inspiration by sharing with people close to them, such as family and very close friends. Currently, only Fitbit distinguishes family from the other connections. Through the “My Family” feature in Fitbit, users can create a family account (Fig. 2), create accounts for kids, and invite other family members or guardians. The other four platforms do not offer this feature. One limitation with the Fitbit family account feature is that one cannot customize data based on individuals, though this may not be a concern when sharing with family members as people are often comfortable sharing detailed information with family [2]. In Apple Activity, users can share their data with family members if each member has the watch. As in the friends’ pattern, sharing with family in Apple Activity is peer to peer, which means that data shared by a user with one family member will not be accessible to the other members. Added family members will be considered as general friends in the remaining three platforms, and thus the visibility and interaction among them is dependent on the platform settings for friends.

Health/Fitness Support Groups Pattern. Seeking advice and accountability related to health and fitness are common goals for sharing information by fitness tracker users. There are currently two methods offered by wearable device platforms for sharing data with health and fitness groups (mostly strangers): within the platform communities and on external fitness communities, such as Strava.

Fitbit, Polar Flow, and Garmin Connect offer users the ability to join and create various health and fitness groups around personal interests, such as weight loss and running. Samsung Health only offers a simple feature to compare step count with users of the same age group, as well as with all users. For Polar Flow and Garmin Connect groups, they can be created using the web service only. These platforms have similar privacy settings for groups, as shown in Table 4. The discoverability of a group is dependent on the controls provided by a platform. Open groups and their posts are visible to all users. Private groups, their posts, and members are not visible to people outside the group, and can members can join through an invitation. Closed groups are similar to private groups, but visibility of posts depends on the platform. For example, a Fitbit closed group, their members, and posts will not be visible to other users. Thus, Fitbit in fact has two options for a group creation: an open or a closed group.

The other method to share fitness tracker data with groups is through external apps, such as Strava. Currently, all platforms except Apple Watch Activity and Samsung Health allow users to connect device data to different external partner apps. Prior versions of Samsung Health enabled users to connect to partner services, but this option is no longer available according to Samsung. Apple Watch Activity users can connect their device data with third parties through the “Watch” app.



< Account My Family •••

GUARDIANS

You
Main Guardian

+ Add Guardians

You are the main guardian of this family, which means you can make other members guardians and create child accounts.

MEMBERS

A A.
Member

+ Invite Members

CHILDREN

+ Create Child Account

Discover Today Community

Fig. 2: Family Feature within Fitbit.

Caregivers Pattern. The examined platforms have no features to share data directly with health providers or to interact with them. Thus, the only method to share self- tracking data with healthcare providers is to have a compatible health provider app with the device platform in order to automatically pull out users’ data. Samsung Health stopped supporting the “Expert” feature within their platform, a service that Samsung said was covered by most health insurance companies, which enabled users to directly contact doctors regarding any issue with their health or fitness data recorded by a device [20]. Apple Watch Activity provides interesting visualizations of health and fitness data because it can integrate with the

TABLE IV: Visibility Controls for Groups.

Level	Fitbit	Apple Activity	Polar Flow	G. Connect	S. Health
Private Group	✓	N/A	✓	✓	N/A
Closed Group	X	N/A	✓	✓	N/A
Open Group	✓	N/A	✓	✓	N/A

Health app, which in turn can integrate with compatible health provider apps. One limitation with Activity is that it does not provide features to capture or track sleep data as the other four platforms do.

Incentive Programs Pattern. Different services that provide monetary incentives for healthy practices can be connected with wearable fitness devices. Only Fitbit and Polar Flow were found to have compatible services that offer financial incentives. For example, Fitbit enables users to connect their accounts with a pharmacy to earn points based on activity level, which can be used as discounts. For Polar Flow, some of the partner services can be connected through the web service only.

Users need to first provide permission to incentive apps to access their data. The examined platforms have different representations regarding how users' data will be accessed by third party apps. In addition, each platform can have different representations based on the type of third-party app (Fig. 3). We found most of the descriptions presented to users by these platforms to be generic, and permission options are less granular. The Fitbit iOS interface, for instance, provides a list of data in a high-level format (e.g., activity and exercises).

Workplaces Pattern. To encourage employees to maintain a healthy lifestyle, some employers offer wellness programs in a workplace. Participated employees will be able to share data collected by their fitness trackers, compare, and compete with each other.

We found two primary methods to automatically share fitness tracker data, mainly step count, in workplaces. The first method is a feature offered by a wearable device company either within the mobile app or in the webpage as a service for employers, commonly called a Corporate Wellness Program. Thus, employees need to use the same fitness tracker brand to participate. This feature is currently supported by Fitbit [6], Polar Flow [17], and Garmin Connect [15]. Managing the privacy of participants depends on the configurations offered by the fitness tracker company. The second method is to simply create a workmate group within a platform, if a group feature is offered. This method has two limitations: first, it is difficult to manage groups of a large size; and again, participants usually need to have the same fitness tracker brand.

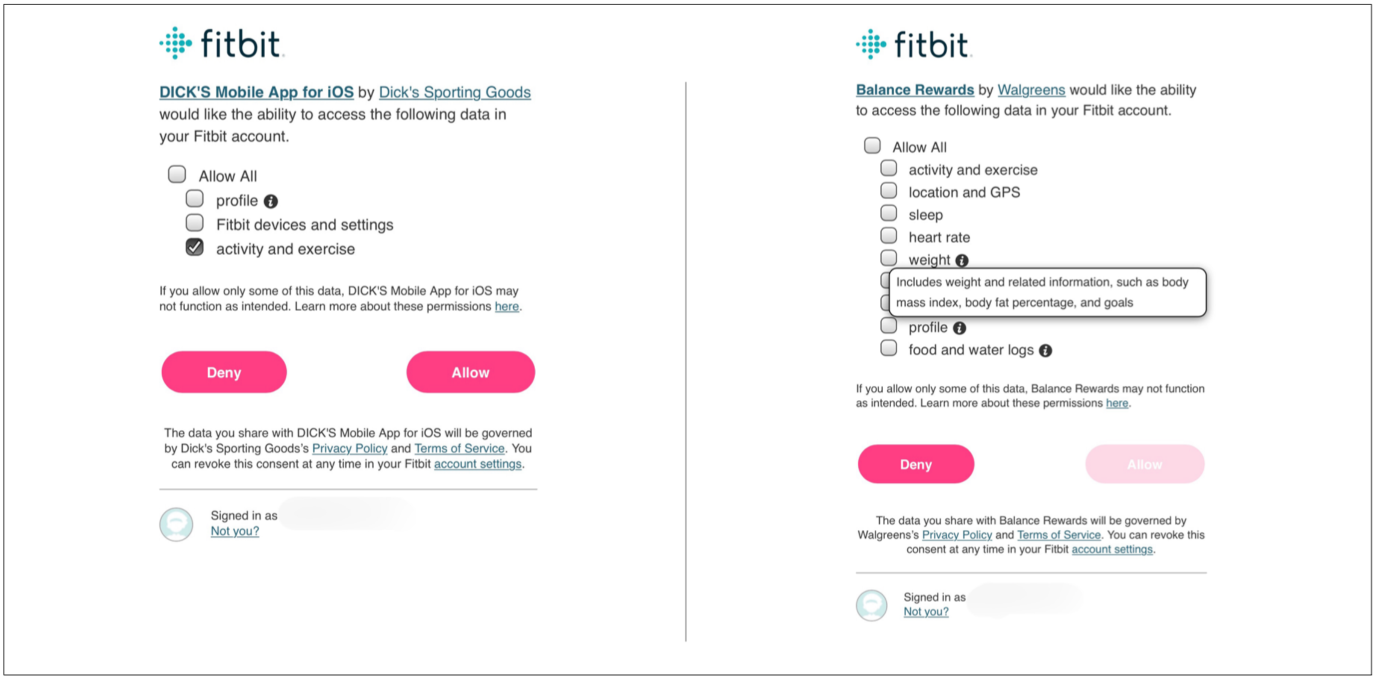
As in the incentive programs pattern, employers can have their own third-party app that can integrate with some wearable device platforms through their Application Programming Interfaces (APIs) to pull out users' data. Thus, the level of access to data depends on a device platform.

B. Data Collection Awareness Mechanisms

The purpose of a wearable fitness device is to automatically collect data and report it to users. All devices have detailed views of the sensed information (e.g., movement data and sleep pattern). Studies indicated that data collected by these sensor devices can be used to infer sensitive information. Therefore, we examined the collection awareness mechanisms of additional information in these platforms. We define data collection awareness mechanisms as any interface notifications (e.g., pop up windows), permission requests, feedback or statements within a device platform that inform users about what personal information will be collected and how it will be used. As a reminder, privacy policies and ToS Agreements are outside the scope of this analysis. In the following paragraphs, we summarize some of these awareness mechanisms in each platform.

One type of sharing that users are made aware of is third party apps. Overall, all platforms that can be connected to external services have similar awareness mechanisms for third parties. Descriptions and lists of data that can be accessed are presented to users in a high-level format (e.g., activity rather than steps, active minutes; sleep rather than sleep time and duration). Fitbit and Polar Flow provide additional contextual information, such as when an app has been approved. In addition, Fitbit provides information about the type of access (read, write) and sometimes a short description of the purpose of collecting data by a third party app. Note that in Polar Flow, this information can only be seen through its web service. Much of the Activity app data, such as access to location, is managed from the Watch app and the phone settings. Garmin Connect users can directly enable/disable phone permissions, such as camera and location information, from the app itself with information by Garmin about what data collected by these systems can be used for.

Another awareness mechanism related to the collection of data is when a user creates an account in these platforms. Some platforms provide users information about the personal details that can be inferred from the data they enter or enable through account creation. Overall, the platforms differ slightly in their mechanism and degree of transparency. For example, the Polar Flow web service has short, yet informative, statements about the information that can be inferred from the data collected from users, such as predicting if a user is normal weight, underweight, or obese based on the entered weight and height. When installing a new device, Garmin Connect presents users with several health and fitness tracking features that can also be enabled from the settings, such as stress level based on heart rate variability, which Garmin stated would be visible to users only. The Apple Watch app provides users with short disclaimers, sometimes with links, about the data that will be collected if users enable certain tracking features. For example, if users click on the "Heart" feature, they will be presented



fitbit

DICK'S Mobile App for iOS by Dick's Sporting Goods would like the ability to access the following data in your Fitbit account.

- □ Allow All
  - □ profile
  - □ Fitbit devices and settings
  - ☑ activity and exercise

If you allow only some of this data, DICK'S Mobile App for iOS may not function as intended. Learn more about these permissions here.

Deny Allow

The data you share with DICK'S Mobile App for iOS will be governed by Dick's Sporting Goods's Privacy Policy and Terms of Service. You can revoke this consent at any time in your Fitbit account settings.

Signed in as [redacted]
Not you?

fitbit

Balance Rewards by Walgreens would like the ability to access the following data in your Fitbit account.

- □ Allow All
  - □ activity and exercise
  - □ location and GPS
  - □ sleep
  - □ heart rate
  - □ weight
  - □ profile
  - □ food and water logs

Includes weight and related information, such as body mass index, body fat percentage, and goals

If you allow only some of this data, Balance Rewards may not function as intended. Learn more about these permissions here.

Deny Allow

The data you share with Balance Rewards will be governed by Walgreens's Privacy Policy and Terms of Service. You can revoke this consent at any time in your Fitbit account settings.

Signed in as [redacted]
Not you?

Fig. 3: Two Data Access Representation by Fitbit for Two Third Party apps.

with several statements with links that describe how heart data can be used to infer additional information.

In terms of notifications, we did not find notifications that deal with privacy in these platforms except those that alert users about friendship requests, likes, or comments by other users.

V. Discussion

Here we discuss gaps and potential design opportunities in relation to the sharing patterns and data collection awareness mechanisms we identified in the platforms we analyzed.

A. Sharing Patterns

Friends. Sharing with connections is the most feature-rich pattern supported by wearable fitness devices. Platforms provide a number of controls for connecting and disclosing information. However, there appear to still be mechanisms that are missing. Specifically, users should be allowed to select which recipient they want to share their fitness data with. Currently, all platforms do not differentiate between connections with respect to their level of relationship with a user. A possible solution is to allow customization similar to Facebook Custom List (i.e., friends, specific friends, acquaintances, etc.). Fitbit also has a limitation in that it does not enable sharing exercise data with all connections in a single click, but a user needs to repeat the action for all connections, which can be tedious. Apple Watch Activity has also room for improvement regarding this mechanism, particularly when data is shared on social media apps. Apple Activity users can only share three abstract rings that represent daily levels of: move, exercise, and stand. Yet, this abstract data does not tell all of the story about one's activity level, and users may desire to share and compare granular details with peers.

Family. One group of people that users commonly feel comfortable sharing with is family. Among the five investigated platforms, only Fitbit provides a family-related feature. However, users' sharing behaviors are dynamic even with close connections, such as family, and the existing Fitbit family feature lacks controls that enable users to change their preferences. We suggest redesigning the family account main interface to enable users to specify their sharing preferences. For instance, users might be allowed to click on a particular family member's picture that takes the user to that member's page, and then a tab could be added that allows users to select what information they want to share with particular members. By making these improvements, we believe that the Fitbit family account would be a model for other platforms to include the family feature.

Health/Fitness Support Groups. Wearables, such as Apple and Samsung Watches are primarily designed to be smart with some of the phone functionalities integrated in them. Therefore, they have fewer considerations for socializing. Incorporating some social features, such as fitness communities and groups in their fitness tracking apps could potentially improve users' wellbeing through competition and accountability. Group creation in Polar Flow and Garmin Connect can currently be managed via their websites. Implementing this feature in the mobile app would be easier and more convenient for users to manage their data. As far as the sharing settings related to fitness groups, there are no controls across all the examined platforms that can allow users to disclose different information with different group members.

Caregivers. People are increasingly utilizing wearable devices for different personal health and fitness goals, such as monitoring diabetes, weight management, injury re covery, etc. Users had dissatisfaction about the lack of support for communication with doctors regarding self-tracking data by the current platforms [2]. Currently, there is no option in any platform to enables users to directly communicate with health providers regarding self-tracking data. Thus, we urge for providing mechanisms that enable integration with health provide systems, while also ensuring that controls are available to protect users' sensitive information. Other features could support composing summary views or downloadable data that are appropriate and customized for caregiving settings.

Incentive Programs. Increasing physical activity through financial incentives is a powerful strategy, but this is may not be without a price. Third party companies that provide these services may utilize users' health and fitness data for research and marketing purposes, which could lead to undesirable inferences about users, including personal identity exposure. In all the examined platforms, companies are allowed to access users' personal data at a high-level (e.g., Fig. 3), which means that they could legally access detailed information without users' awareness. Users should be able to control all dimensions of their information. We noticed that while users do have some granular controls and awareness, there are currently no mechanisms to enable users to audit what information a third-party has accessed.

Workplaces. Workplace health campaigns are popular and could be supported by wearable fitness trackers. Only three platforms integrate a workplace wellness feature in their platforms currently which mostly collects step count. Individuals who join these programs may do so in response to social pressure. While step count may not be of a huge concern for participants in these programs, such data may provide an impression about a person's health and fitness lifestyle. Thus, designers of these features should provide flexible controls that enable participants in these workplace programs to change their sharing preferences anytime and to accommodate different interpersonal boundaries. Aside from these interpersonal concerns, there is a wide concern that data collected in these programs could be used for secondary purposes, for example by employers or health insurance companies [16]. As of now, privacy policies appear to be the only possible mechanism to understand whether such data use could occur. Additional mechanisms within the app could be useful as well.

B. Data Collection Awareness

Data collection awareness mechanisms can help users understand what information about them can be used, and thus make informed privacy decisions. Apart from lengthy privacy policies and ToS agreements, we conclude that there are inadequate awareness mechanisms, both active and passive, in wearable fitness device platforms. Those few mechanisms that are already implemented, such as links to descriptions of how particular sensors work to measure some personal data, are mostly overwhelming or unseen for users. For example, Polar Flow provides short statements in the user account information about how certain data users provided can be used to disclose additional information (e.g., if a user is normal weight, underweight, or obese based on height and weight). Yet, users would only view this information once, while creating an account. Rather, awareness mechanisms can be simplified in a way that could engage users in order to increase their awareness. For example, platform interfaces could display how certain pieces of activity information work together, such as showing how heart rate rhythms change and calories are burned while walking.

Another common limitation in the data collection mechanisms we found in these platforms is third party authorization, which are implemented to collect users' data at high levels. These mechanisms can be re-designed by adding granularity as well as contextual details, such as when a particular app was approved by a user and how frequently the app has accessed data. Lastly, the current platforms also fail in terms of privacy notifications, such as those that remind users about their sharing practices with third party apps. For example, a user could be reminded if they still want to keep connecting an app that has been given permission for a long period of time (e.g., more than 6 months). We suggest implementing these notifications periodically to help users in controlling the privacy of their personal information.

VI. CONCLUSION

Platforms of wearable fitness devices could be redesigned to satisfy users' sharing goals and privacy need. In this paper, we examined the sharing and privacy mechanisms of five poplar wearable device platforms for tracking fitness. We presented a set of taxonomies based on sharing patterns, boundary controls, and data collection awareness mechanisms. Our findings show similar mechanisms among the examined platforms. We also identified some design limitations where we believe improvements could be made in these platforms to further users' ability to useful share their data while still protecting their privacy. We consider this study to be an initial step of a future work that aims to design sharing and privacy solutions in wearable fitness device platforms.

ACKNOWLEDGMENT

We thank Najran University, Saudi Arabia, for funding the first author to conduct this research.

REFERENCES

[1] Aktypi, A., Nurse, J. R., & Goldsmith, M. Unwinding Ariadne's identity thread: Privacy risks with fitness trackers and online social networks. In Proceedings of the 2017 on Multi- media Privacy and Security, pp. 1-11 (2017).

[2] Alqhatani, A., & Lipford, H. R. (2019). "There is nothing that I need to keep secret": Sharing Practices and Concerns of Wearable Fitness Data. In Fifteenth Symposium on Usable Pri- vacy and Security (SOUPS 2019).

[3] Bahirat, P., He, Y., Menon, A., Knijnenburg, B.: A data-driven approach to developing iot privacy-setting interfaces. In: 23rd International Conference on Intelligent User Interfaces, pp. 165–176. ACM (2018).

[4] Business Insider. “Global Wearable Computing Devices Market (2020 to 2025) - Growth, Trends & Forecasts.” https://markets.businessinsider.com/news/stocks/global-wearable-computing-devices-market-2020-to-2025-growth-trends-forecasts-1029337176# Accessed: 2020-06-08.

[5] Dong, M., Chen, L., & Wang, L. Investigating the User Behaviors of Sharing Health-and Fitness Related Information Generated by Mi Band on Weibo. International Journal of Hu- man–Computer Interaction, 1-14 (2018).

[6] Fitbit. https://healthsolutions.fitbit.com/employers/. Accessed: 2019-10-28.

[7] Fritz, T., Huang, E. M., Murphy, G. C., & Zimmermann, T. 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, pp. 487-496 (2014).

[8] Gui, X., Chen, Y., Caldeira, C., Xiao, D., & Chen, Y. When fitness meets social networks: Investigating fitness tracking and social practices on werun. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, pp. 1647-1659 (2017).

[9] Karr-Wisniewski, P., Wilson, D., & Richter-Lipford, H. A new social order: Mechanisms for social network site boundary regulation. In Americas Conference on Information Systems, AMCIS. 2011.

[10] Kreitzberg, D. S. C., Dailey, S. L., Vogt, T. M., Robinson, D., & Zhu, Y. What is Your Fitness Tracker Communicating?: Exploring Messages and Effects of Wearable Fitness De- vices. Qualitative Research Reports in Communication, 17(1), 93-101 (2016).

[11] Kröger,J.Unexpected inferences from sensor data:a hidden privacy threat in the internet of things. In IFIP International Internet of Things Conference, pp. 147-159 (2019). Springer,Cham.

[12] Lampinen, A. Interpersonal boundary regulation in the context of social network services. 2014.

[13] Lupton, D. Quantifying the body: monitoring and measuring health in the age of mHealth technologies. Critical Public Health, 23(4), 393-403. (2013).

[14] Mare,S.,Girvin,L.,Roesner,F.,& Kohno,T.Consumer smart homes:Where we are and where we need to go. In Proceedings of the 20th International Workshop on Mobile Com- puting Systems and Applications, pp. 117-122 (2019).

[15] Pai., A. “Garmin offers employers wellness portal, health challenges Garmin.” MobiHealth News. https://www.mobihealthnews.com/39362/garmin-offers-employers-wellness-portal health-challenges. Accessed: 2020-06-01.

[16] Peppet, S. R. Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent. Tex. L. Rev., 93, 85 (2014).

[17] Polar.com. https://www.polar.com/us-en/b2b_products/corporate_fitness. Accessed: 2020- 05-16.

[18] Prasad, A., Sorber, J., Stablein, T., Anthony, D., & Kotz, D. Understanding user privacy preferences for mhealth data sharing. mHealth: Multidisciplinary verticals, 545-569 (2014).

[19] Raij, A., Ghosh, A., Kumar, S., & Srivastava, M. Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 11-20 (2011).

[20] Samsung.com. https://www.samsung.com/uk/support/mobile-devices/what-is-samsung- health-ask-an-expert-powered-by-babylon/. Accessed: 2020-06-04.

[21] Statista. ”Market share of wearables unit shipments worldwide by vendor from 2014 to 2019”. https://www.statista.com/statistics/515640/quarterly-wearables-shipments-worldwide-market-share-by-vendor/ Accessed: 2021-02-01.

[22] Torre, I., Sanchez, O. R., Koceva, F., & Adorni, G. Supporting users to take informed deci sions on privacy settings of personal devices. Personal and Ubiquitous Computing, 22(2), 345-364 (2018). Springer. https://doi.org/10.1007/s00779-017-1068-3

[23] Witte, A. K., & Zarnekow, R. Is Open Always Better?-A Taxonomy-based Analysis of Plat form Ecosystems for Fitness Trackers.

[24] Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), 2728-2742 (2014).