Journal of Ambient Intelligence and Humanized Computing - preprint

What data are smartphone users willing to share with researchers?

Designing and evaluating a privacy model for mobile data collection apps

Felix Beierle · Vinh Thuy Tran · Mathias Allemand · Patrick Neff · Winfried Schlee · Thomas Probst · Johannes Zimmermann · Rüdiger Pryss

Received: 2 January 2019 / Accepted: 5 June 2019

This work was done in the context of project DYNAMIC (http://www.dynamic-project.de) (grant No 01IS12056), which is funded as part of the Software Campus initiative by the German Federal Ministry of Education and Research (BMBF).

Felix Beierle
Service-centric Networking
Telekom Innovation Laboratories
Technische Universität Berlin
Berlin, Germany
E-mail: beierle@tu-berlin.de

Vinh Thuy Tran
Technische Universität Berlin
Berlin, Germany
E-mail: vinh.t.tran@campus.tu-berlin.de

Mathias Allemand
Department of Psychology
University of Zurich
Zurich, Switzerland
E-mail: mathias.allemand@uzh.ch

Patrick Neff
Clinic and Policlinic for Psychiatry and Psychotherapy
University of Regensburg
Regensburg, Germany
E-mail: patrick.neff@uzh.ch

Winfried Schlee
Clinic and Policlinic for Psychiatry and Psychotherapy
University of Regensburg
Regensburg, Germany
E-mail: winfried.schlee@tinnitusresearch.org

Thomas Probst
Department for Psychotherapy and Biopsychosocial Health
Danube University Krems
Krems, Austria
E-mail: thomas.probst@donau-uni.ac.at

Johannes Zimmermann
Department of Psychology
University of Kassel
Kassel, Germany
E-mail: jz@uni-kassel.de

Abstract Context-aware applications stemming from diverse fields like mobile health, recommender systems, and mobile commerce potentially benefit from knowing aspects of the user's personality. As filling out personality questionnaires is tedious, we propose the prediction of the user's personality from smartphone sensor and usage data. In order to collect data for researching the relationship between smartphone data and personality, we developed the Android app TYDR (Track Your Daily Routine), which tracks and records smartphone data and utilizes psychometric personality questionnaires. With TYDR, we track a larger variety of smartphone data than many other existing apps, including metadata on notifications, photos taken, and music played back by the user. Based on the development of TYDR, we introduce a general context data model consisting of four categories that focus on the user's different types of interactions with the smartphone: *physical* conditions and activity, *device* status and usage, *core functions* usage, and *app* usage. On top of this, we developed the Privacy Model for Mobile Data Collection Applications (PM-MoDaC) specifically tailored for apps that are related to the collection of mobile data, consisting of nine proposed privacy measures. We present the implementation of all of those measures in TYDR. Our experimental evaluation is based on data collected with TYDR during a two-month period. We find evidence that our users accept our proposed privacy model. Based on data about granting TYDR all or no Android system permissions, we find evidence that younger users tend to be less willing to share their data

Rüdiger Pryss
Institute of Databases and Information Systems
Ulm University
Ulm, Germany
E-mail: ruediger.pryss@uni-ulm.de

(average age of 30 years compared to 35 years). We also observe that female users tend to be less willing to share data compared to male users. We did not find any evidence that education or personality traits are a factor related to data sharing. TYDR users score higher on the personality trait *openness to experience* than the average of the population, which we assume to be evidence that the type of app influences the user base it attracts in terms of average personality traits.

Keywords ubiquitous computing · context-aware computing · mobile computing · psychometrics · sensor data · privacy

1 Introduction

The modern smartphone is a small personal computer that is used for a large variety of tasks in different contexts. A multitude of sensors and an omnipresent internet connectivity make apps aware of the user's context. This context can be used to personalize or contextualize applications, for example, by recommending something based on the current time or location. Oftentimes, the context that is taken into consideration is limited to directly measurable factors like location, battery status, or installed apps.

Having additional data about the user's personality could improve context-aware systems from different domains, e.g., mobile health, personalization and recommendations, or mobile commerce. Mobile health applications could benefit from personality data for the diagnosis or treatment of patients (e.g., Pryss et al. 2015; Roche et al. 2014; Zimmermann et al. 2019; Pryss et al. 2018). Context-aware recommender systems may benefit from personality data, as was shown in a recent study with the MovieLens recommender system (Karumur et al. 2017). The importance of personality for the attitude towards advertising and mobile commerce is highlighted for example in Myers et al. (2010), Zhou and Lu (2011), and Matz et al. (2017).

Psychological research suggests that there are links between personality traits and everyday preferences (Beierle et al. 2017). With a smartphone, we will be able to track different types of data that might reflect the user's personality: the smartphone's sensors can track the user's physical context and the operating system can track the user's interaction with the smartphone and its apps. We argue that, after collecting data labeled with the personality of the user, we might be able to predict (aspects of) the user's personality from sensor and usage data without applying questionnaires (Hinds and Joinson 2019).

In order to collect data to perform a study analyzing the relationship between smartphone data and personality, we developed the Android app TYDR (Track Your Daily Routine). TYDR collects smartphone sensor and usage data as well as applies standardized psychological questionnaires to the user. In Beierle et al. (2018b), we highlighted some aspects about the development process of the app, relating to the implementation of sensor data collection and some privacy aspects.

In this paper, based on our research with TYDR, we first focus on what type of smartphone data is available. As this data is highly sensitive, we then introduce a privacy model. We evaluate our approach, finding evidence that our proposed privacy model is accepted by our users. The main contributions of this paper are:

- We propose a general context data model for smartphone applications that focuses on the user's interaction with the phone.
- We introduce the privacy model PM-MoDaC for apps relating to mobile data collection.
- We give an overview of the implementation of the introduced privacy model in the Android app TYDR.
- We perform an extensive evaluation of the proposed privacy model based on data collected with TYDR and evaluate what type of users are willing to share which data.

This paper is a revised and largely extended version of Beierle et al. (2018a). We fully implemented our app TYDR, released it on Google Play, and collected data from users during a two-month period. We report on our extensive statistical evaluation of the collected data. The conducted user study was approved by the ethics commission of the Technical University of Berlin (BEI_01_20180115). The remainder of this paper is structured as follows. In Section 2, we review related work, showing that none of the existing projects take into account all the available data sources present on current smartphones. We present a general model of context data for smartphone applications in Section 3 and introduce our privacy model PM-MoDaC in Section 4. We show the implementation of PM-MoDaC in TYDR in Section 5. In Section 6, we evaluate our experiences collecting data with TYDR while employing PM-MoDaC, and in Section 7, we conclude and point out future work.

2 Related Work and Study Planning

In Table 1, we give an overview of related studies that correlated sensor and/or smartphone usage data with user information related to personality. Some of those studies have been conducted with feature phones, be-

Table 1 Overview of data sources and user information that were correlated in previous studies.

Data Sources	User Information	Property	References
Bluetooth, calls, sms, calling profiles, application usage (pre-smartphone)	personality traits	static	Chittaranjan et al. (2011, 2013)
calls, sms, changing ringtones and wallpapers (pre-smartphone)	personality traits	static	Butt and Phillips (2008)
location	personality traits	static	Chorley et al. (2015); Kim et al. (2018)
technology usage times	personality traits	static	Grover and Mark (2017)
calls, sms, location	personality traits	static	de Montjoye et al. (2013)
installed apps	personality traits	static	Xu et al. (2016)
app usage	personality traits	static	Stachl et al. (2017)
calls, sms, proximity data, weather	daily stress	dynamic	Bogomolov et al. (2014)
accelerometer, Bluetooth, location	emotions	dynamic	Rachuri et al. (2010)
location	depressive states	dynamic	Canzian and Musolesi (2015)
email, sms, calls, websites, location, app usage	mood	dynamic	LiKamWa et al. (2013)

fore the advent of smartphones (Chittaranjan et al. 2011, 2013; Butt and Phillips 2008). The *data sources* given in the table differ in their level. For example, accelerometer data is low level sensor data, while the current activity (e.g., walking, in car, etc.) or a daily step count is higher level sensor data that utilizes accelerometer data. The available data sources depend on the used mobile OS and on the available libraries and Software Development Kits (SDKs). In the table, we also list the sources mentioned in the cited papers. There might be some steps in between low level sensor data and the user's personality, like estimating the user's sleep pattern utilizing low level sensor data like phone lock/unlock events. For overviews related to determining higher level features from lower level sensor data see Harari et al. (2016), Harari et al. (2017), or Mohr et al. (2017).

The ground truth for *user information* is typically assessed via self-report methods, i.e., questionnaires. Often, the authors of the studies describe use cases to illustrate what the predicted user information could be meaningful for. Most of the studies aim at use cases related to mobile health or context-aware recommender systems, e.g., recommending new apps based on the personality correlated with already installed apps (Xu et al. 2016). Some studies go further than correlating data with the personality of the user. The StudentLife project, for example, collected sensor data and queried student participants with a variety of questionnaires to predict mental health and academic performance (Wang et al. 2014, 2015, 2017). In Sariyska et al. (2018), the authors studied the molecular genetic underpinnings of individual differences in human social behavior. Based on automatically collected call and movement logs, they determined the social network of the users, without having to rely on self-assessment by the user.

In the *property* column of Table 1, we distinguish related studies as being *static* or *dynamic*. A static system will look for information such as personality traits that are relatively stable. A dynamic study will try to find correlations between sensor/usage data and changing aspects about the user, for example, mood or stress level (LiKamWa et al. 2013; Bogomolov et al. 2014).

There are some additional projects that are related to our research. Sensus (Xiong et al. 2016), LiveLabs (Jayarajah et al. 2016), and AWARE (Ferreira et al. 2015) aim at providing researchers with frameworks for conducting research related to collected sensor/smartphone usage data. As far as the papers and website indicate, none of these frameworks provide support for collecting music and photo metadata, which we enable with TYDR.

Most of the cited studies are interested in personality traits of the user. The most prominent structural model of individual differences in personality traits is the Big Five model (McCrae and John 1992), consisting of the trait domains *openness to experience*, *conscientiousness*, *extraversion*, *agreeableness*, and *neuroticism*. In order to assess the personality traits, we use the Big Five Inventory 2 (BFI-2) questionnaire (Danner et al. 2016; Soto and John 2017). Moreover, the expression of personality traits fluctuates within persons across time (Fleeson 2001). For example, a person who scores high on neuroticism will experience negative mood more often than other people, but may still vary considerably in the experience of negative mood across time, e.g., depending on situational circumstances. This within-person variability of emotions and behaviors is captured by the term *personality states*. In order to register those aspects, we utilize the PDD (Personality Dynamics Diary) questionnaire, which captures the user's experience of daily situations and behaviors (Zimmermann et al. 2019). With the results of a study with TYDR, we will

investigate to what extend we can make daily predictions about personality states based on context data.

3 Categorization of Context Data

In broad terms, Dey defines context as something which is relevant to an application (2001). Often, context is categorized into *device*, *user*, *physical* surrounding and activity, and *temporal* aspects (Yurur et al. 2014). However, this does not reflect the users' interaction with the smartphone. For example, the number of pictures taken or which apps a user is using may yield important information about his/her context. A user taking many pictures and using map applications might be at an unfamiliar place that he/she enjoys.

In Table 2, we introduce a general context data model for the categorization of context data for smartphone applications. The four categories are *physical* conditions and activity, *device* status and usage, *core functions* usage, and *app* usage. Furthermore, an additional technical category constitutes the explicit permission by the user in order to allow an app to access data from the given source. This has important implications, e.g., for answering the question if it is possible to develop a library for personality prediction that does not require explicit permissions.

Physical conditions and activity deal with the physical context of the user that is not related to the interaction with the smartphone. Here, sensors deliver data without the user interacting with the phone, e.g., location or taken steps. The ambient light sensor typically offers data only when the screen is active, so when the user is interacting with the phone. However, as its data is related to the physical context, i.e., the light level of the environment of the user, we regard it as part of the *physical* category.

The category ***device*** status and usage designates data that is related to the status and the connectivity of the smartphone. This comprises screen/lock state, headphone connection status, battery level and charging status as well as Wifi and Bluetooth connectivity.

Core functions usage deals with the users' interaction with core functionalities of the phone, regardless of which specific apps they are using for it. The core functions comprise calling, music listening, taking photos, and dealing with notifications.

The fourth category is ***app*** usage, dealing with data about the usage and traffic of specific apps. Notifications fit both in the *core functions* and the *apps* categories because they can be related to either.

The *permission* column is based on the permission system introduced with Android 6.0 (API 23). Weather is given in parenthesis because it can only be collected if the location is available, so it is bound to the location permission. Music is given in parenthesis as well. Most major music player apps or music streaming apps automatically broadcast metadata about music that the user is currently listening to. The broadcast events can be received by any app that subscribes as a listener (Beierle et al. 2016). However, for Spotify, such broadcasting has to be activated manually.

Table 2 Context data model for the categorization of context data for smartphone applications. The last column indicates if an explicit user permission is required (Android).

	Category				**Permission**
	Physical	Device	Core functions	Apps	
location	•				•
weather	•				(•)
ambient light sensor	•				
ambient noise level	•				•
accelerometer	•				
gyroscope	•				
activity	•				
steps	•				
screen and lock state		•			
headphone un-/plug		•			
battery and charging		•			
Wifi		•			
Bluetooth		•			
calls metadata			•		•
music metadata			•		(•)
photos metadata			•		•
notifications metadata			•	•	•
app usage				•	•
app traffic				•	•

There is additional data that could be gathered from mobile phones, e.g., touch patterns or touch intensity (cf., e.g., Carneiro et al. 2017). However, data points are only available when the developed app itself is in the foreground, not whenever any other app is being used. Thus, it might be difficult or impossible to get meaningful data for purposes like personality prediction.

In general, our context data model can be helpful for the development of any context-aware service, e.g., in the areas of ubiquitous computing and mobile social networking (Beierle et al. 2015; Beierle 2018). After collecting data, we have to analyze to what extend the quality of the context data varies between the variety of different available Android devices. Our context data categorization allows to address different specific questions based on our research question regarding the prediction of the user's personality. Specific questions are, for example, whether the physical context alone can predict personality, how meaningful metadata is, or how accurate the prediction can be if the user did not give any explicit permissions.

4 PM-MoDaC – Privacy Model for Mobile Data Collection Applications

As we are dealing with highly sensitive data, privacy concerns should have a high priority. In this section, we present a comprehensive overview of measures that can be taken to protect user privacy. To the best of our knowledge, we are the first to provide such a comprehensive privacy model for applications related to mobile data collection.

Of the reviewed related work, only one paper provides some details about the processes and measures taken to ensure user privacy (Kiukkonen et al. 2010). Some works do not give any technical details about privacy protection (Canzian and Musolesi 2015; Bogomolov et al. 2014) or openly state that they disregarded the issue, e.g., Rachuri et al. (2010): "privacy is not a major concern for this system, since all users voluntarily agree to carry the devices for constant monitoring." In their study about technologies about self-reporting of emotions, Fuentes et al. report similar findings (2017): most of the reviewed work did not mention privacy at all. If there is information given about privacy protection, it is typically not very detailed and usually only covers some of the aspects given in the following privacy model.

Our **Privacy Model for Mobile Data Collection Applications (PM-MoDaC)** comprises the nine privacy measures (PM) given in Table 3 which are described in the following.

Table 3 The nine privacy measures of PM-MoDaC.

(A)	User Consent
(B)	Let Users View Their Own Data
(C)	Opt-out Option
(D)	Approval by Ethics Commission / Review Board
(E)	Random Identifiers
(F)	Data Anonymization
(G)	Utilize Permission System
(H)	Secured Transfer
(I)	Identifying Individual Users Without Linking to Their Collected Data

(A) User Consent Before installing the app, the user should be explained what data exactly is being collected and for what purpose. These are typical aspects covered in a privacy policy that the user has to agree to before using an app. The aspect of *user consent* is mentioned in Kiukkonen et al. (2010) and Stachl et al. (2017).

(B) Let Users View Their Own Data Only Kiukkonen et al. (2010) discuss this aspect of privacy protection. By letting the users see the data that is being collected, they can make a more informed decision about sharing it.

(C) Opt-out Option The possibility of opting-out is only mentioned in Wang et al. (2014). Especially after viewing their own data (see previous point), users might decide that they no longer want to use the app or participate in the study.

(D) Approval by Ethics Commission / Review Board Psychological or medical studies typically require prior approval by an ethics commission or review board. Three of the related works state that such approval was given for their studies (Canzian and Musolesi 2015; Ferreira et al. 2015; Jayarajah et al. 2016). This aspect of privacy protection is more on a meta-level, as an ethics commission / review board might check the other points mentioned in this privacy model.

(E) Random Identifiers When starting an app, often a login is required. This poses the privacy risk of linking highly sensitive data with personal details, e.g., the user's Facebook account details if a Facebook account was used to log in. Two related studies describe using random identifiers (Wang et al. 2014; Xu et al. 2016). This point relies on the type of study being conducted. Investigating the relationship between collected sensor data and, for example, the number of Facebook friends, would probably require the user to login via Facebook. On a technical level for the Android system, an ID provided by the Google Play Services proved itself suitable as a random ID (cf. Beierle et al. (2018b)).

(F) Data Anonymization This aspect is mentioned most commonly in the related work (Kiukkonen et al. 2010; Chittaranjan et al. 2011, 2013; LiKamWa et al. 2013; Ferreira et al. 2015; Jayarajah et al. 2016). If details are given, they usually describe how one-way hash functions are used to obfuscate personally identifiable data like telephone numbers, Wifi SSIDs, or Bluetooth addresses.

TYDR only stores clear text data where it is necessary for the research purpose. Our context categorization from Section 3 helps to analyze why metadata will suffice in most cases. Consider notifications for example. Depending on the application, they might contain highly sensitive data, e.g., the message content of a messenger application. The content of the notification is not relevant for our research purpose. The app name that caused the notification however is, as one could easily imagine a relationship between, e.g., the personality trait *extraversion* and the frequency of chat/messaging app notifications.

An additional point to consider regarding data anonymization is where the anonymization happens. In Jayarajah et al. (2016), the authors describe how the anonymization is taking place on the backend that the data is being sent to, before being stored. In TYDR, the anonymization process is taking place on the device itself, before storing to the local device and before sending data to the backend. The backend consists of server, application, and database. So, even if our backend was compromised, the attacker would only be able to access data that is already anonymized.

(G) Utilize Permission System This point is specifically related to the Android permission system that was introduced with Android 6.0 (cf. Section 3). By itself, it can already make the users more aware of what data/sensor is being accessed by an application. The designers of an application still have influence over how they make use of the system though. Requesting all permissions at the first start of an app, e.g., gives the user little insight about what each permission is used for. Instead, the app should request a permission at the point where it is needed and explain to the user what the accessed data source is being used for.

(H) Secured Transfer The point of having secured data transfer between mobile device and backend is explicitly mentioned in Wang et al. (2014) and Ferreira et al. (2015). An alternative way is to only locally collect data and ask users in a lab session to bring their phone and copy the data then. Such an approach would severely limit the possible scope of a study.

(I) Identifying Individual Users Without Linking to Their Collected Data In psychological studies, it is common that users are compensated with university course credit points, get paid to participate, or have the chance to win money/vouchers in a raffle after study completion. In order to contact the study participants, contact information is needed, which might contradict PM E. In order to alleviate this concern, we developed a process for identifying individual users without linking to their collected data on the backend (Beierle et al. 2018b). In short, the process consists of storing contact data separately from the collected smartphone data and letting the app check the requirements for successful study completion, in our case the daily completion of the PDD questionnaire. This way, we can create incentives for users to install and use the app while simultaneously preserving user privacy.

In Li et al. (2018), the authors also deal with the often contradicting requirements of privacy and user incentivization. Here, the authors propose a system with automatic pay-outs. In this case, technological advancement is faster than bureaucratic processes, which sometimes still require manual approval or handwritten signatures.

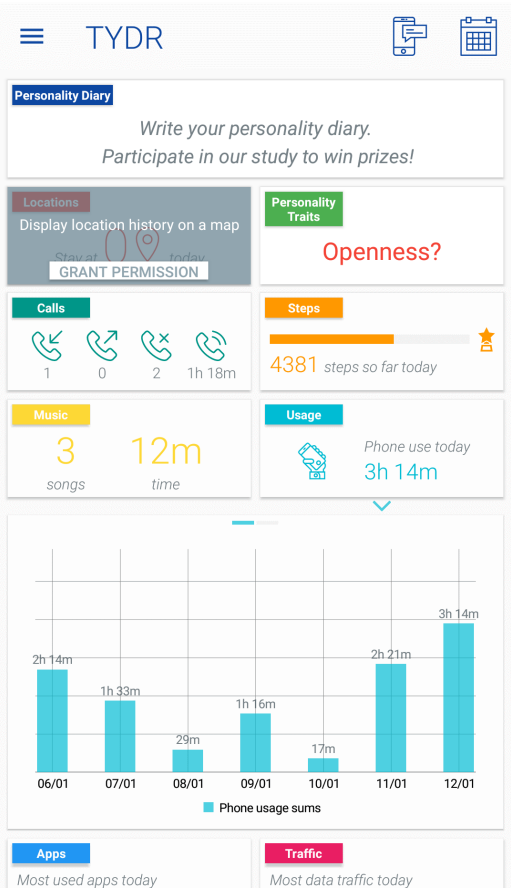

Fig. 1 Main screen of TYDR.

5 Implementation of the Privacy Model PM-MoDaC in TYDR

With TYDR, to the best of our knowledge, we are the first to implement a privacy model comprising all nine privacy measures listed in Section 4. The visualization of the data that is collected about the user is TYDR's core feature (PM B). The ethics commission of Technische Universität Berlin approved of using TYDR in a psychological study (PM D).

Figure 1 shows TYDR's main screen and how it visualizes the collected data in a tile-based layout. Each tile shows a daily summary of one data type. By touching a tile, a larger tile appears below with a weekly summary, see for example the phone usage tile in the figure. Users can opt-out via the contact form from the sidebar menu (PM C). In Figure 2, we show a diagram of the main processes in the TYDR app. The person icon in a process signifies that the user is actively doing something. All other processes are part of the app and do not require user interaction. Starting TYDR for the first time, the user has to confirm the terms and the privacy policy (cf. PM A). Only then the five processes of the app are started. Note that there is no login process, the systems uses a random unique identifier (PM E).

At the bottom of Figure 2, we show that the app starts the data collection (Process 4). The data collection engine already anonymizes the data before storing it (PM F). The uploading via a secure connection (PM H) is started after the app registered itself with the backend. The upload process is repeated every 24 hours (Process 5).

The process at the top of the figure shows the main menu of TYDR (Process 1), also cf. Figure 1. From here, the user can grant permissions (cf. Table 2 and Figure 1; PM G), which influences the data collection. The user can also fill out the general (demographic information) and the personality traits questionnaire (*Personality Traits* tile in Figure 1). TYDR offers a permanent notification, displaying information on the lockscreen and the notification bar (Process 2). The data to be displayed can be configured by the user via the second icon from the right in the top (Figure 1). The tracking of personality states via the PDD questionnaire is designed to be optional (Process 3). Configuring the PDD questionnaire via the *Personality States* tile (Figure 1), the user can (de-)activate this feature. In order to collect data labeled with personality states, we conducted a study where users commit to turning this feature on for a certain period of time. The registration for this study takes into account PM I.

6 Evaluation

In order to gain insights about mobile data collection apps and the proposed privacy model, we released TYDR on Google Play in mid-November 2018 and collected the data this evaluation is based on. In order to advertise TYDR, we printed flyers that were distributed at the universities of the authors of this paper. Most TYDR installations happened after a German website that deals with Android-related content reported about new apps including TYDR. Looking at PM-MoDaC, there are some aspects that the user cannot interact with, i.e., PM B, D, E, F, H, and I. With the remaining

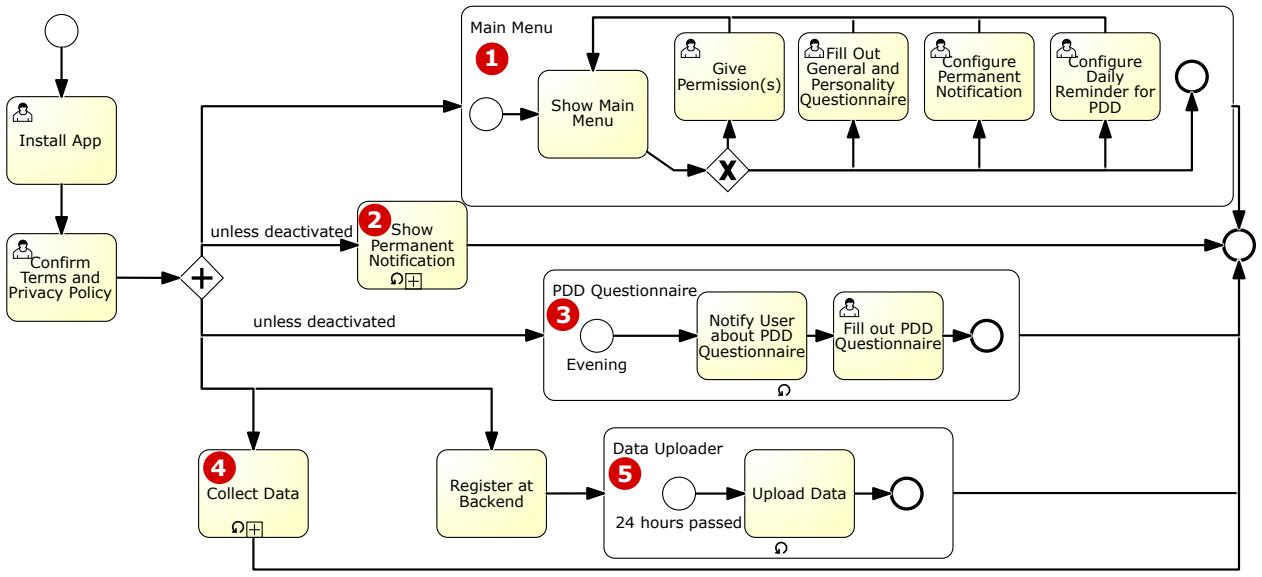

Fig. 2 Process diagram for our smartphone sensor and usage data tracking app TYDR.

three aspects, PM A (User Consent), C (Opt-out Option), and G (Permission System), the user can interact with. To be more precise, the user can accept or decline the terms and conditions and the privacy policy (PM A). The user can choose to opt-out and request his/her data to be deleted. Furthermore, the user can determine which permissions he/she grants to TYDR.

In this section, we address the following research questions (RQ):

RQ1 What kind of data can researchers expect when they publish an app related to mobile data collection?

RQ2 Is there evidence regarding user acceptance of PM-MoDaC?

RQ3 In what way are user characteristics related to granted permissions?

Data Sets TYDR was released on Google Play mid-November 2018. For the two months period between 12 November 2018 and 17 January 2019, Google reports 3010 installations. In our database, we have 2876 users, and, after data cleaning, we have 1560 users with valid information about their permissions settings. Data set DS1 contains these users. Out of these users, 634 filled out a demographic questionnaire (data set DS2). Out of those, 461 also filled out the Big Five personality traits questionnaire (data set DS3). Note that this makes DS3 a subset of DS2 and DS2 a subset of DS1: DS3 $\subset$ DS2 $\subset$ DS1. In Table 4, we give an overview about the data sets and how the users interacted with the permission system (PM G).

Table 4 Data sets used in the evaluation. About the users in DS1, we have valid permission information. The users in DS2 filled out the demographic questionnaire, while users in DS3 also filled out the personality questionnaire, hence we have DS3 $\subset$ DS2 $\subset$ DS1.

Granted Perm.	**DS1**	**DS2**	**DS3**
all perm.	660 (42%)	387 (61%)	287 (62%)
only some perm.	344 (22%)	162 (26%)	123 (27%)
no perm.	556 (36%)	85 (13%)	51 (11%)
sum	1560	634	461

For DS2, demographic information is available. 83% (527) of TYDR users are male, while 17% (107) are female. The mean age of the TYDR users is 33.93 years (SD: 12.43). For the users in DS3, we provide the average for the Big Five personality traits scores in Table 5. We compare the values with the population averages given in Danner et al. (2016) and give a standardized effect size (Cohen's d). The biggest difference in comparison with the population average is that TYDR users score higher on the trait *openness to experience*. We assume that TYDR by its nature as an app that displays smartphone statistics might attract users with such a personality pattern. Considering the ubiquity of smartphones, we assume that the average smartphone user resembles the average of the population. The results shown in Table 5 could then be evidence that the user base acquired by an app depends on the type of the app (RQ1).

(A) User Consent There is a difference of 134 users between the number of installations reported by Google (3010) and the number of users in our database (2876). Only after consenting to the terms and conditions as well as the privacy policy, a connection to our backend is established (cf. Figure 2). After the connection is established, an entry in our database is created. This yields a rate of 95.5% of users that accepted our terms and conditions as well as our privacy policy. The remaining 134 users could have never opened the app after installation, there could have been an error during the connection with our backend, or they had concerns about the given terms and policy.

We have data about 778 users that confirmed terms and policy and gave the permission to access their app usage statistics. For those users, we can see how long they spend on the *Welcome* activity of TYDR. This activity is shown to the user when he/she starts the app for the first time. It consists of two screens. The first shows the TYDR logo and contains a brief description of what TYDR does. On the second screen, the terms and conditions and the privacy policy are displayed, they have a combined length of overall around 1300 words. The average time spend in this activity is only 10 seconds (SD: 23.6), clearly not enough to read the texts of the privacy policy and the terms and conditions. Assuming an average reading speed of 200 words per minute, reading the full texts would take about 6.5 minutes. While it is possible to (re-)read both texts at any later point from within a menu in the app, our data confirms the stereotype of the user not reading the privacy policy and blindly confirming. We assume that those with high concerns about sharing data will not have installed TYDR in the first place. Overall, privacy does not seem to be a concern for those users that want to install and use the app (RQ2).

(C) Opt-out Option Only one user withdrew his or her data from the study. According to our understanding of the GDPR, each service has to offer the option to delete all of a user's data. In that respect, this is not a feature unique to TYDR, but should be a feature available in any service (offered in the EU). In TYDR,

Table 5 Average Big Five personality trait scores (scale: 1-5) of TYDR users (DS3) in comparison with the population averages given in Danner et al. (2016); including the differences between the means and Cohen's d effect size.

	TYDR			Population Average			Difference	Cohen's d
Personality Traits	Mean	SD	Cronbach's Alpha	Mean	SD	Cronbach's Alpha		
openness to experience	3.70	0.63	0.78	3.38	0.64	0.84	+0.32	+0.50
conscientiousness	3.37	0.64	0.81	3.67	0.62	0.87	-0.30	-0.48
extraversion	3.16	0.67	0.82	3.22	0.63	0.86	-0.06	-0.10
agreeableness	3.64	0.54	0.72	3.76	0.51	0.81	-0.12	-0.24
neuroticism	2.85	0.82	0.89	2.72	0.67	0.88	+0.13	+0.19

we explicitly described the opt-out option in the privacy policy. However, we did not implement a dedicated button for this. This could have created a bias towards users not requesting the deletion of their data.

(G) Permission System Looking into what users granted TYDR which permissions can give us insight into what concerns our users have regarding which data source (RQ1, RQ3). The permissions used in TYDR are:

- storage
- location
- call log
- app usage
- notifications

For the last two, Android opens an extra confirmation page for the user because apps that are granted these permission can access especially sensitive data.

To reduce complexity, in the following, we looked into users that granted either all or no permissions. To test for demographic and psychological differences between TYDR user groups giving all or no permissions, we compared permission groups with regard to age, gender, education, and personality traits and facets. For the comparison of the mean age and personality traits and facets scores between groups we applied Student's t-tests, whereas Wilcoxon ranksum tests were used to test for differences in education. Finally, a Chi-Square test was used to test for differential distributions between the genders. The statistical tests performed were two-tailed and the significance level was set to $p < 0.05$. All analyses were conducted using R.

There are some aspects to consider when interpreting the results: Users that did not fill out the demographic or personality questionnaire because of privacy concerns are not reflected in the following statistics, simply because their data is not available. Filling out the questionnaires itself could be related to concerns about sharing data as well, i.e., a user could decide not to answer the questionnaires because of privacy concerns. The difference to the automatically collected context data is that the demographic and personality data is static and not updated. Furthermore, not giving permissions does not necessarily mean the user had privacy concerns, there could be other reasons which we will mention in the following.

Note on DS1. 30% (471) of our users did not fill out any questionnaire and did not give any permission (i.e., the cardinality of $\{user \text{ in DS1} \setminus \text{DS2} \mid user \text{ did not give any permissions}\}$, cf. Table 4, is 471). We assume this group of users might not have had any interest in using the app after starting it.

Gender. The Chi-Square test indicates that there is a relationship between gender and having given no or all permissions ($p = 0.001$). 12% of our male users did not give any permissions, while 22% of the female users did not give any permissions, see Table 6. 64% of male users granted all permissions, while only 48% of female users granted all permissions. This could be evidence that female users are less willing to share their data. An alternative explanation could be that the gender difference might also be based on a difference in interest: Maybe some female users installed the app, had a look at it, and decided they do not want to use it because they are not interested.

Table 6 Gender and permission settings (DS2).

Granted Perm.	**female**	**male**	**sum**
all perm.	51 (48%)	336 (64%)	387 (61%)
only some perm.	32 (30%)	130 (25%)	162 (26%)
no perm.	24 (22%)	61 (12%)	85 (13%)
sum	107	527	634

Age. The mean age of the users giving no permissions is lower that that of those giving all permissions (29.75 years vs. 34.87 years; $p = 0.0002$). The violin plot in Figure 3 shows the age distribution for each users group giving all or no permission, divided by gender. The size indicates the sample size and the dot gives the mean for the user group. We observe that TYDR's female users

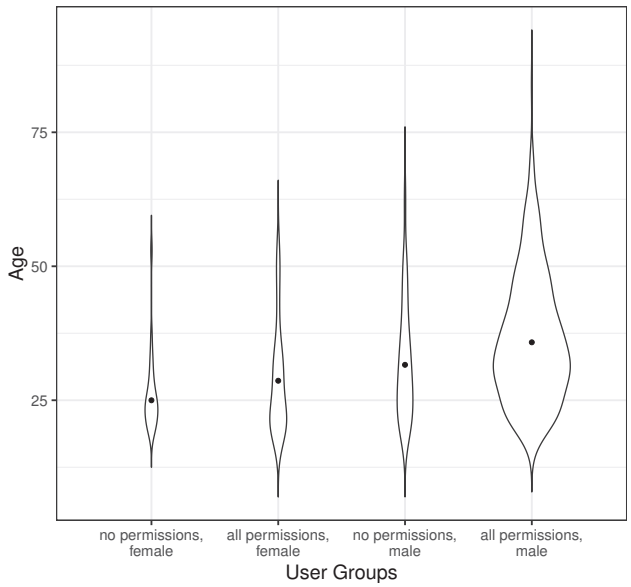

Fig. 3 Age distribution showing the age of TYDR users giving all or no permission. The size of the plot indicates the sample size and the dot indicates the mean (DS2).

are younger on average. For both male and female users, the average age is lower in the group of those users giving no permissions. There are a few ways to interpret these results. The younger people are, the more likely it is that they grew up with smartphones from an earlier age. This group of users might be more prone to installing and quickly uninstalling apps without using every feature. Another interpretation could be that younger users tend to have more technical background knowledge and tend to have a heightened sensitivity towards data privacy. If our observation is related to privacy concerns, it is consistent with López et al. (2017), in which the authors found that young people (16-25 in this case) are most concerned about privacy issues.

Education. In our demographic questionnaire, we asked for the highest completed level of education. We did not find any statistically significant association between level of education and giving all or no permissions.

Personality. We do not observe any difference with respect to personality traits of the user and giving all or no permissions (all p-values > 0.1). With the personality questionnaire used, the five personality dimensions can each be separated into three facets. Looking into those, we observe that the facet *intellectual curiosity*, part of the trait *openness to experience*, is higher in those who did not give any permissions ($p = 0.005$). However, this does not necessarily mean that intellectually curious people are less willing to share their data or have more privacy concerns. It could be that the group of users that filled out the personality questionnaire but did not grant any system permissions, consisted of users that were more curious about their personality profile and less about their smartphone usage statistics. In Table 7 we present the means and standard deviations of the personality traits and facets scores for the two TYDR users groups giving all and no permissions.

Table 7 Big Five personality traits and facets scores for TYDR users giving all or no permissions (DS3).

	All Perm.		**No Perm.**	
Pers. Traits and Facets	Mean	SD	Mean	SD
openness to experience	3.67	0.64	3.83	0.64
aesthetic sensitivity	3.83	0.91	3.55	1.06
creative imagination	3.71	0.81	3.72	0.83
intellectual curiosity	3.96	0.75	4.23	0.60
conscientiousness	3.39	0.63	3.36	0.60
organization	3.42	0.90	3.36	0.90
productiveness	3.22	0.83	3.15	0.72
responsibility	3.53	0.69	3.57	0.73
extraversion	3.14	0.65	3.33	0.80
assertiveness	3.23	0.80	3.50	0.89
energy level	3.34	0.80	3.48	0.98
sociability	2.83	0.88	3.00	0.97
agreeableness	3.62	0.53	3.67	0.63
compassion	3.73	0.70	3.82	0.79
respectfulness	3.90	0.64	3.86	0.78
trust	3.23	0.74	3.32	0.72
neuroticism	2.88	0.81	2.92	0.86
depression	2.74	0.99	2.74	0.98
anxiety	3.18	0.89	3.24	0.92
emotional volatility	2.73	0.96	2.80	1.07

Discussion / Results In Di Matteo et al. (2018), the authors surveyed patients if they would be willing to use an app related to assessing their mental health disorder. While most where willing to install, willingness to give certain permissions was lower. The authors report that 68% of the surveyed patients may be willing to agree to have the state of their screen monitored by such an app. At least on Android, most likely, users might not even notice which apps are already doing this, as in order to do so, no explicit permission is required from the user (cf. Table 2). On average, the surveyed people were least willing to grant access to share audio recordings and SMS content – content TYDR does not collect in anticipation of such unwillingness. In contrast to using a survey, we performed analyses on data collected with an actually deployed app. Furthermore, the target audience in our case was very broad, user might have different concerns about apps relating to mental health.

In DS2[1], only 26% of users granted only some permissions while 61% granted all of them (cf. Table 6). This could indicate that users might actually be willing to grant more permissions than they might indicate in a survey.

In general, not granting certain permissions to an app could relate to privacy concerns / concerns about data sharing, but could also just be evidence for a lack of interest in the app. Overall, we feel we found quite a lot of users to try and use TYDR. Almost all of the feedback we received from our users was about certain features and not related to privacy or data usage.

From this and from the data analysis we conducted, we found evidence for the following points that address RQ1-3:

- PM-MoDaC seems to be a valid approach to dealing with privacy in mobile data collection apps.
- Younger users tend to be more concerned about privacy / data sharing.
- Female users seem to tend to be less willing to share data.
- Education does not seem to be a factor related to data sharing.
- Personality traits do not seem to be a factor related to data sharing.
- Depending on the type of app, the user base might be biased towards certain personality traits.

We consider these aspects as being helpful for other researchers that conduct studies with mobile applications. More specifically, our revealed aspects can be seen as indicators what kind of data can be expected in this context.

7 Conclusion and Future Work

Context-aware applications can potentially benefit from data relating to the user's personality. This includes rather static personality traits and more dynamic personality states. To be able to conduct a study on the relationship between smartphone sensor and usage data and the user's personality, we developed the Android app TYDR. It tracks smartphone data and utilizes standardized personality questionnaires. TYDR tracks more types of data than existing related apps, including metadata on notifications, photos taken, and music listened to.

We developed a general context data model for smartphone applications, highlighting the different kinds of interactions with the smartphone: *physical* conditions and activity, *device* status and usage, *core functions* usage, and *app* usage. We further developed the privacy model PM-MoDaC comprising nine proposed measures that can be taken to ensure user privacy in apps related to mobile data collection. On top of this, we presented the implementation of those nine measures for our Android app TYDR.

We conducted a study with TYDR and collected data from users in a two-month period. Performing extensive statistical analyses, we especially observed the users' behavior when granting TYDR Android systems permissions to access specific data sources. Comparing granting no or all permissions, we observe that age of those that tend to be less willing to share their data is lower, 30 years compared to 35 years. Furthermore, we observe that female users tend to be less willing to share data compared to male users. Analyzing the educational background and the personality trait scores of the users, we do not observe any statistically relevant pattern with respect to sharing data. Comparing the average personality trait scores from TYDR users to the population average, we find some evidence that the type of app influences the user base with respect to the average user personality. At least when starting the app for the first time, users do not spend a lot of time on reading the terms and conditions and the privacy policy – on average 10 seconds for about 1300 words. Based on our users' behavior with the permission system and based on user feedback from within the app and via email, we consider PM-MoDaC as widely accepted by our users.

Future work includes data analyses relating to the prediction of the user's personality from smartphone data. This could comprise one prediction for personality traits and daily predictions for personality states. Based on our findings, we plan to develop a library for the unobtrusive prediction of aspects of the user's personality that can be utilized in context-aware applications. The study results will have to show which permissions will be necessary for such a library and what categories of context will be the best predictors. Regarding the privacy model, there are further questions to research, e.g., how to convey the privacy measures implemented to the user, especially if he or she is not tech-savvy.

Acknowledgements We are grateful for the support provided by Daniel Lenz, Sakshi Bansal, Marcel Müller, Soumya Siladitya Mishra, and Sarjo Das. We also thank all TYDR users.

[1] We consider DS2 instead of DS1 here, as DS1 contains several users that probably never used or intended to use the app; see *Note on DS1* above.

References

Beierle F (2018) Do You Like What I Like? Similarity Estimation in Proximity-based Mobile Social Networks. In: Proc. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom), IEEE, pp 1040–1047, DOI 10.1109/TrustCom/BigDataSE.2018.00146

Beierle F, Göndör S, Küpper A (2015) Towards a Three-tiered Social Graph in Decentralized Online Social Networks. In: Proc. 7th International Workshop on Hot Topics in Planet-Scale mObile Computing and Online Social neTworking (HotPOST), ACM, pp 1–6, DOI 10.1145/2757513.2757517

Beierle F, Grunert K, Göndör S, Küpper A (2016) Privacy-aware Social Music Playlist Generation. In: Proc. 2016 IEEE International Conference on Communications (ICC), IEEE, pp 5650–5656, DOI 10.1109/ICC.2016.7511602

Beierle F, Grunert K, Göndör S, Schlüter V (2017) Towards Psychometrics-based Friend Recommendations in Social Networking Services. In: 2017 IEEE International Conference on AI & Mobile Services (AIMS), IEEE, pp 105–108, DOI 10.1109/AIMS.2017.22

Beierle F, Tran VT, Allemand M, Neff P, Schlee W, Probst T, Pryss R, Zimmermann J (2018a) Context Data Categories and Privacy Model for Mobile Data Collection Apps. Procedia Computer Science 134:18–25, DOI 10.1016/j.procs.2018.07.139

Beierle F, Tran VT, Allemand M, Neff P, Schlee W, Probst T, Pryss R, Zimmermann J (2018b) TYDR – Track Your Daily Routine. Android App for Tracking Smartphone Sensor and Usage Data. In: 2018 ACM/IEEE 5th International Conference on Mobile Software Engineering and Systems (MOBILESoft '18), ACM, pp 72–75, DOI 10.1145/3197231.3197235

Bogomolov A, Lepri B, Ferron M, Pianesi F, Pentland AS (2014) Daily Stress Recognition from Mobile Phone Data, Weather Conditions and Individual Traits. In: Proc. 22nd ACM International Conference on Multimedia, ACM, MM '14, pp 477–486, DOI 10.1145/2647868.2654933

Butt S, Phillips JG (2008) Personality and self reported mobile phone use. Computers in Human Behavior 24(2):346–360, DOI 10.1016/j.chb.2007.01.019

Canzian L, Musolesi M (2015) Trajectories of Depression: Unobtrusive Monitoring of Depressive States by Means of Smartphone Mobility Traces Analysis. In: Proc. of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp), ACM, UbiComp '15, pp 1293–1304, DOI 10.1145/2750858.2805845

Carneiro D, Pinheiro AP, Novais P (2017) Context acquisition in auditory emotional recognition studies. Journal of Ambient Intelligence and Humanized Computing 8(2):191–203, DOI 10.1007/s12652-016-0391-2

Chittaranjan G, Blom J, Gatica-Perez D (2011) Who's Who with Big-Five: Analyzing and Classifying Personality Traits with Smartphones. In: Proc. 2011 15th Annual International Symposium on Wearable Computers, IEEE, pp 29–36, DOI 10.1109/ISWC.2011.29

Chittaranjan G, Blom J, Gatica-Perez D (2013) Mining large-scale smartphone data for personality studies. Personal and Ubiquitous Computing 17(3):433–450, DOI 10.1007/s00779-011-0490-1

Chorley MJ, Whitaker RM, Allen SM (2015) Personality and location-based social networks. Computers in Human Behavior 46(Supplement C):45–56, DOI 10.1016/j.chb.2014.12.038

Danner D, Rammstedt B, Bluemke M, Treiber L, Berres S, Soto C, John O (2016) Die deutsche Version des Big Five Inventory 2 (BFI-2). In: Zusammenstellung Sozialwissenschaftlicher Items und Skalen, DOI 10.6102/zis247

de Montjoye YA, Quoidbach J, Robic F, Pentland A (2013) Predicting Personality Using Novel Mobile Phone-Based Metrics. In: SBP, Springer, pp 48–55, DOI 10.1007/978-3-642-37210-0_6

Dey AK (2001) Understanding and Using Context. Personal Ubiquitous Comput 5(1):4–7, DOI 10.1007/s007790170019

Di Matteo D, Fine A, Fotinos K, Rose J, Katzman M (2018) Patient Willingness to Consent to Mobile Phone Data Collection for Mental Health Apps: Structured Questionnaire. JMIR Mental Health 5(3), DOI 10.2196/mental.9539

Ferreira D, Kostakos V, Dey AK (2015) AWARE: Mobile Context Instrumentation Framework. Frontiers in ICT 2, DOI 10.3389/fict.2015.00006

Fleeson W (2001) Toward a Structure-and Process-Integrated View of Personality: Traits as Density Distributions of States. Journal of Personality and Social Psychology 80(6):1011–1027, DOI 10.1037/0022-3514.80.6.1011

Fuentes C, Herskovic V, Rodríguez I, Gerea C, Marques M, Rossel PO (2017) A systematic literature review about technologies for self-reporting emotional information. Journal of Ambient Intelligence and Humanized Computing 8(4):593–606, DOI 10.1007/s12652-016-0430-z

Grover T, Mark G (2017) Digital Footprints: Predicting Personality from Temporal Patterns of Technology Use. In: Proc. 2017 ACM Intl. Joint Conference on Pervasive and Ubiquitous Computing and Proc. 2017 ACM Intl. Symposium on Wearable Computers, ACM, UbiComp '17, pp 41–44, DOI 10.1145/3123024.3123139

Harari GM, Lane ND, Wang R, Crosier BS, Campbell AT, Gosling SD (2016) Using Smartphones to Collect Behavioral Data in Psychological Science: Opportunities, Practical Considerations, and Challenges. Perspectives on Psychological Science 11(6):838–854, DOI 10.1177/1745691616650285

Harari GM, Müller SR, Aung MS, Rentfrow PJ (2017) Smartphone sensing methods for studying behavior in everyday life. Current Opinion in Behavioral Sciences 18(Supplement C):83–90, DOI 10.1016/j.cobeha.2017.07.018

Hinds J, Joinson A (2019) Human and Computer Personality Prediction From Digital Footprints. Current Directions in Psychological Science 28(2):204–211, DOI 10.1177/0963721419827849

Jayarajah K, Balan RK, Radhakrishnan M, Misra A, Lee Y (2016) LiveLabs: Building In-Situ Mobile Sensing & Behavioural Experimentation TestBeds. In: Proc. 14th Annual International Conference on Mobile Systems, Applications, and Services, ACM, MobiSys '16, pp 1–15, DOI 10.1145/2906388.2906400

Karumur RP, Nguyen TT, Konstan JA (2017) Personality, User Preferences and Behavior in Recommender systems. Information Systems Frontiers pp 1–25, DOI 10.1007/s10796-017-9800-0

Kim SY, Koo HJ, Song HY (2018) A study on estimation of human personality from location visiting preference. Journal of Ambient Intelligence and Humanized Computing 9(3):629–642, DOI 10.1007/s12652-017-0459-7

Kiukkonen N, Blom J, Dousse O, Gatica-Perez D, Laurila J (2010) Towards rich mobile phone datasets: Lausanne data collection campaign. In: Proc. ACM Intl. Conf. on

Pervasive Services (ICPS)
Li Y, Zhao Y, Ishak S, Song H, Wang N, Yao N (2018) An anonymous data reporting strategy with ensuring incentives for mobile crowd-sensing. Journal of Ambient Intelligence and Humanized Computing 9(6):2093–2107, DOI 10.1007/s12652-017-0529-x
LiKamWa R, Liu Y, Lane ND, Zhong L (2013) MoodScope: Building a Mood Sensor from Smartphone Usage Patterns. In: Proc. 11th Annual International Conference on Mobile Systems, Applications, and Services, ACM, MobiSys '13, pp 389–402, DOI 10.1145/2462456.2464449
López G, Marín G, Calderón M (2017) Human aspects of ubiquitous computing: A study addressing willingness to use it and privacy issues. Journal of Ambient Intelligence and Humanized Computing 8(4):497–511, DOI 10.1007/s12652-016-0438-4
Matz SC, Kosinski M, Nave G, Stillwell DJ (2017) Psychological targeting as an effective approach to digital mass persuasion. Proceedings of the National Academy of Sciences 114(48):12714–12719, DOI 10.1073/pnas.1710966114
McCrae RR, John OP (1992) An Introduction to the Five-Factor Model and Its Applications. Journal of Personality 60(2):175–215
Mohr DC, Zhang M, Schueller SM (2017) Personal Sensing: Understanding Mental Health Using Ubiquitous Sensors and Machine Learning. Annual Review of Clinical Psychology 13:23–47, DOI 10.1146/annurev-clinpsy-032816-044949
Myers SD, Sen S, Alexandrov A (2010) The moderating effect of personality traits on attitudes toward advertisements: A contingency framework. Management & Marketing 5(3):3–20
Pryss R, Reichert M, Langguth B, Schlee W (2015) Mobile Crowd Sensing Services for Tinnitus Assessment, Therapy, and Research. In: 2015 IEEE International Conference on Mobile Services (MS), IEEE, pp 352–359, DOI 10.1109/MobServ.2015.55
Pryss R, Probst T, Schlee W, Schobel J, Langguth B, Neff P, Spiliopoulou M, Reichert M (2018) Prospective crowdsensing versus retrospective ratings of tinnitus variability and tinnitus–stress associations based on the TrackYourTinnitus mobile platform. International Journal of Data Science and Analytics pp 1–12, DOI 10.1007/s41060-018-0111-4
Rachuri KK, Musolesi M, Mascolo C, Rentfrow PJ, Longworth C, Aucinas A (2010) EmotionSense: A Mobile Phones Based Adaptive Platform for Experimental Social Psychology Research. In: Proc. 12th ACM Intl. Conference on Ubiquitous Computing (UbiComp), ACM, UbiComp '10, pp 281–290, DOI 10.1145/1864349.1864393
Roche MJ, Pincus AL, Rebar AL, Conroy DE, Ram N (2014) Enriching Psychological Assessment Using a Person-Specific Analysis of Interpersonal Processes in Daily Life. Assessment 21(5):515–528, DOI 10.1177/1073191114540320
Sariyska R, Rathner EM, Baumeister H, Montag C (2018) Feasibility of Linking Molecular Genetic Markers to Real-World Social Network Size Tracked on Smartphones. Frontiers in Neuroscience 12, DOI 10.3389/fnins.2018.00945
Soto CJ, John OP (2017) The next Big Five Inventory (BFI-2): Developing and assessing a hierarchical model with 15 facets to enhance bandwidth, fidelity, and predictive power. Journal of Personality and Social Psychology 113(1):117–143, DOI 10.1037/pspp0000096
Stachl C, Hilbert S, Au JQ, Buschek D, De Luca A, Bischl B, Hussmann H, Bühner M (2017) Personality Traits Predict Smartphone Usage. European Journal of Personality 31(6):701–722, DOI 10.1002/per.2113
Wang R, Chen F, Chen Z, Li T, Harari G, Tignor S, Zhou X, Ben-Zeev D, Campbell AT (2014) StudentLife: Assessing Mental Health, Academic Performance and Behavioral Trends of College Students Using Smartphones. In: Proc. 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp), ACM, UbiComp '14, pp 3–14, DOI 10.1145/2632048.2632054
Wang R, Harari G, Hao P, Zhou X, Campbell AT (2015) SmartGPA: How Smartphones Can Assess and Predict Academic Performance of College Students. In: Proc. 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp), ACM, pp 295–306, DOI 10.1145/2750858.2804251
Wang R, Chen F, Chen Z, Li T, Harari G, Tignor S, Zhou X, Ben-Zeev D, Campbell AT (2017) StudentLife: Using Smartphones to Assess Mental Health and Academic Performance of College Students. In: Mobile Health, Springer, pp 7–33, DOI 10.1007/978-3-319-51394-2_2
Xiong H, Huang Y, Barnes LE, Gerber MS (2016) Sensus: A Cross-platform, General-purpose System for Mobile Crowdsensing in Human-subject Studies. In: Proc. 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp), ACM, UbiComp '16, pp 415–426, DOI 10.1145/2971648.2971711
Xu R, Frey RM, Fleisch E, Ilic A (2016) Understanding the impact of personality traits on mobile app adoption – Insights from a large-scale field study. Computers in Human Behavior 62(Supplement C):244–256, DOI 10.1016/j.chb.2016.04.011
Yurur O, Liu C, Sheng Z, Leung V, Moreno W, Leung K (2014) Context-Awareness for Mobile Sensing: A Survey and Future Directions. IEEE Communications Surveys Tutorials 18(1):1–28, DOI 10.1109/COMST.2014.2381246
Zhou T, Lu Y (2011) The Effects of Personality Traits on User Acceptance of Mobile Commerce. International Journal of Human–Computer Interaction 27(6):545–561, DOI 10.1080/10447318.2011.555298
Zimmermann J, Woods WC, Ritter S, Happel M, Masuhr O, Jaeger U, Spitzer C, Wright AGC (2019) Integrating structure and dynamics in personality assessment: First steps toward the development and validation of a personality dynamics diary. Psychological Assessment 31(4):516–531, DOI 10.1037/pas0000625

Additional Information

Bibliographic Data F. Beierle, V. T. Tran, M. Allemand, P. Neff, W. Schlee, T. Probst, J. Zimmermann, and R. Pryss, “What data are smartphone users willing to share with researchers? Designing and evaluating a privacy model for mobile data collection apps,” *Journal of Ambient Intelligence and Humanized Computing* (2019). https://doi.org/10.1007/s12652-019-01355-6

Pre-print from https://beierle.de

Online at https://doi.org/10.1007/s12652-019-01355-6 and https://rdcu.be/bHn0r

Authors

Felix Beierle

Vinh Thuy Tran

Mathias Allemand

Patrick Neff

Winfried Schlee

Thomas Probst

Johannes Zimmermann

Rüdiger Pryss

BibTeX

```
@article{BeierleJAIHC2019,
title = {{What data are smartphone users willing to share with researchers? Designing and evaluating a privacy model for mobile data collection apps}},
author = {Beierle, Felix and Tran, Vinh Thuy and Allemand, Mathias and Neff, Patrick and Schlee, Winfried and Probst, Thomas and Zimmermann, Johannes and Pryss, R\"udiger},
journal = {{Journal of Ambient Intelligence and Humanized Computing}},
publisher = {Springer},
year = {2019},
doi = {10.1007/s12652-019-01355-6}
}
```