Understanding Privacy Risks and Perceived Benefits in Open Dataset Collection for Mobile Affective Computing

HYUNSOO LEE, KAIST, South Korea
SOOWON KANG, KAIST, South Korea
UICHIN LEE*, KAIST, South Korea

Collecting large-scale mobile and wearable sensor datasets from daily contexts is essential in developing machine learning models for enabling everyday affective computing applications. However, there is a lack of knowledge on data contributors' perceived benefits and risks in participating in open dataset collection projects. To bridge this gap, we conducted an in-situ study on building an open dataset with mobile and wearable devices for affective computing research (N = 100, 4 weeks). Our study results showed that a mixture of financial and altruistic benefits was important in eliciting data contribution. Sensor-specific risks were largely associated with the revelation of personal traits and social behaviors. However, most of the participants were less concerned with open dataset collection and their perceived sensitivity of each sensor data did not change over time. We further discuss alternative approaches to promote data contributors' motivations and suggest design guidelines to alleviate potential privacy concerns in mobile open dataset collection.

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

Additional Key Words and Phrases: Privacy, Risk-Benefit Assessment, Open Dataset, Mobile and Wearable Computing, Affective Computing

ACM Reference Format:
Hyunsoo Lee, Soowon Kang, and Uichin Lee. 2022. Understanding Privacy Risks and Perceived Benefits in Open Dataset Collection for Mobile Affective Computing. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 6, 2, Article 61 (June 2022), 26 pages. https://doi.org/10.1145/3534623

1 INTRODUCTION

There is a growing interest in leveraging mobile and wearable sensors for continuous and passive collection of sensor data from our daily lives (e.g., sleep patterns, social interaction). Such interests can be well observed in the general populations' recent interest in sensor-enabled devices and applications (e.g., physical health tracking apps), research communites' and industries' attempt to collect a vast amount of data for application domains such as digital healthcare [39]. Collected data contribute to research that attempts to understand relationships between people's daily behaviors and user states of interest. One promising area is affective computing or emotional intelligence. Using the dataset collected from multiple sensors, for example, we can develop machine learning models for detecting and interpreting an individual's mental state and design health intervention services (e.g., stress detection and just-in-time intervention) [15, 54, 97, 107].

*Corresponding author.

Authors' addresses: Hyunsoo Lee, hslee90@kaist.ac.kr, KAIST, Daejeon, South Korea; Soowon Kang, sw.kang@kaist.ac.kr, KAIST, Daejeon, South Korea; Uichin Lee, uclee@kaist.ac.kr, KAIST, Daejeon, South Korea.

2474-9567/2022/6-ART61 $15.00
https://doi.org/10.1145/3534623

Despite the promise of such multimodal sensor datasets, only a handful of studies have released open datasets (e.g., the StudentLife project [97], and the Tesserae project [60]). The release of such large-scale, in-the-wild datasets for public use is expected to benefit relevant research communities, and even the general public once commercially available applications are developed. Specifically, we believe that open dataset collection with mobile and wearable devices will make significant contribution to ubiquitous computing research because the large volume of behavioral and contextual data across multiple sensors can be used to develop and evaluate in-situ psychological state inference algorithms [2, 25, 99].

With this background, it is imperative to facilitate open dataset collection practice. Open dataset collection and its application often call for "the more the better," which requires a large volume of data from more participants for high-performance predictive models. To increase the number of participants and make them more cooperative along the data collection projects, reducing risks (i.e., privacy concerns) and identifying participants' potential benefits (i.e., participation motives) are important prerequisites. In terms of risks, collected sensor readings may pose potential privacy threats (e.g., accelerometer data revealing participants' current activities [49], gait recognition data revealing participants' identity [24]), endangering privacy of the participants and even end-users of the technology [19]. There are even potential ethical risks in the models built from the collected dataset; e.g., emotion detection algorithms could be inaccurate or biased, leading to psychological and physical harms [22]. Thus, risk-benefit assessment is a critical process as it ultimately affects participants' attitudes and behaviors toward the overall data collection and its public release.

Although understanding privacy concerns associated with personal data [45, 78] and participant motives (e.g., financial incentives [41, 71]) have been popular research topics in HCI studies, both have been studied individually and in different contexts. We find that risk-benefit assessment in the context of multimodal sensor data collection for building an open dataset – particularly for research purposes — is yet to catch the attention of the ubiquitous computing community. In terms of privacy, we also find that prior studies have mainly focused on a single sensor channel and its derived privacy concerns [18, 21], whereas an in-depth investigation of each sensor and specific concerns in an extensive range of data items is relatively under-explored.

Therefore, we conducted a large-scale in-the-wild investigation to explore participants' general attitudes and privacy concerns in building a mobile sensor dataset, which is dedicated to developing affective computing applications (e.g., mood detection). Through the theoretical lens of a well-known behavioral theory in privacy and a mixed-method (i.e., survey and interview) approach, we identified factors that are associated with participants' attitudes toward in-the-wild open dataset collection. We present findings from a four-week study with 100 college students, who participated in an open dataset collection project that involves both an extensive range of sensor data collected from both mobile and wearable devices.

From our exploratory study, we found that leveraging both financial and altruistic motives (e.g., willingness to contribute to a community) is important in eliciting participants' data contribution. In terms of privacy, our in-depth interview results show that participants expressed sensor-specific "intuitive concerns" because of the potential revelation of personal traits and social behaviors (e.g., calls, texts, app usage, and GPS). In assessing such risks, participants' concerns were centered around potential judgment/categorization of a person and a sense of surveillance.

Despite such sensor-specific concerns, most participants are largely carefree about potential privacy risks. Given a choice on data release preferences, 85 participants consented to the complete release of their collected data, while only 15 requested for selective release (i.e., partly excluding personally sensitive data). Also, most participants reported low levels of perceived sensitivity to each collected sensor data, which did not change over time. Regarding such contradictory patterns, we provide detailed explanations to understand participant behaviors. The contributions of this study are as follows:

- We deepen our understanding of data contributors' motives and privacy concerns toward open dataset collection for affective computing research, which typically involves an extensive range of mobile, wearable, and self-reported data (i.e., psychological status data) collected in-the-wild.
- We characterize various types of privacy concerns in relation to specific sensor data types and report participants' perceived sensitivity to each sensor data type.
- We discuss alternative approaches to promote data contributors' motivations and suggest design guidelines for future studies to alleviate potential privacy concerns in open mobile dataset collection.

To the best of our knowledge, our work is the first to conduct a large-scale study in-the-wild to explore diverse factors that play a role in shaping participants' acceptance of open dataset collection. With increasing interest in open dataset practice and concerns, we provide novel insights on the design of future open dataset collection campaigns.

2 BACKGROUND AND RELATED WORK

Several streams of HCI and ubiquitous computing research have explored the possibility of sensor data collection and users' perceptions towards privacy within a variety of contexts. Below, we situate each of these areas with respect to our study.

2.1 Mobile Sensor Data Collection and Public Release

First, we provide an overview of previous studies on mobile and wearable sensor data collection. The early stages of in-the-field mobile and wearable sensor data collection studies focused on areas such as user activity sensing [12, 21], context inference [26, 30], and identification of users' mobile device usage [93]. Most of these studies were smartphone-based and focused on single behavior tracking, such as location and activity [21]. Moreover, the data collection from most studies were not publicly available, though some datasets were selectively released upon request.

More recently, there has been a growing interest in using mobile phones and wearable devices (e.g., smart bands and smartwatches) to consistently and passively collect comprehensive behavioral sensor data, which can provide an authentic and continuous source of an individual's behaviors and digital footprints [39]. Accordingly, such potentials are opening up new areas of research across diverse application domains by leveraging multiple streams of in-the-wild data sources, such as, everyday behavior [89, 90], user preferences [86], physical activities [88], personal productivity [60], emotions [54, 107], mental wellness [15, 104], sleep [42], and physical health [10].

Among the application domains, researchers have been particularly interested in smart healthcare. Emerging studies have shown that massive amounts of continuously collected by smartphones and wearables in daily living can be repurposed to identify behavioral biomarkers (e.g., social interaction, sleep patterns related to health issues) and build statistical models that can predict the risk of diseases (e.g., heart diseases [10, 96], psychiatric disorders [33]); which is also known as '*digital phenotyping*.' [39]

Furthermore, the results of mobile and wearable sensing studies have progressively been capturing features that are indicative of one's emotions and mental health states [70, 107] or behavioral symptoms of major mental disorders (e.g., depression and schizophrenia) [69]. In particular, digital behavioral markers such as sleep patterns and circadian rhythms have demonstrated significant correlations with one's mental health such as depressive symptoms [15, 97]. The StudentLife project at Dartmouth [97] revealed that students' sleep hours, bluetooth encounters and conversation hours are related to depressive symptoms. A rich body of related studies [18, 29, 80, 104] has proven the feasibility and reliability of identifying behavioral symptoms of mental health (e.g., depression, anxiety and bipolar disorder) by tracking smartphone usage and device sensors.

These studies are closely related to prior studies that modeled users' emotion/cognitive states and mental health states by using mobile and wearable sensor data collected in-the-wild. The application domains generally

belong to the field of affective computing or emotional intelligence, which aims to build data-driven models (e.g., mood-detection algorithms [70]) or relevant systems or services (e.g., real-time interventions [87, 94, 95]) by detecting and interpreting one's mental state (e.g., mood, attention, stress, and depression) based on a variety of data sources.

Despite ongoing active research and the outlined potentials, the availability of mobile and wearable sensor datasets collected *in-the-wild* is currently very limited. Existing affective computing and emotion intelligence datasets are mostly collected in the lab setting [1, 70]. There are only a few in-the-wild open datasets such as StudentLife [97] and the Tesserae project [60]. Our work contributes to the body of existing knowledge on the privacy concerns of open dataset collections for affective computing.

2.2 Privacy Behavior and Risk-Benefit Assessment

For open dataset practice to be facilitated, deepening our understanding of the behavioral intentions of data contributors in data collection and release is imperative. Because participants' attitudes—be they optimistic or pessimistic—will inevitably affect data collection and release, user-centric investigations are required to shed more light on current data practice in the domain. Thus, we review overarching privacy theories that are essential for understanding participants' behavioral tendencies with respect to our study.

2.2.1 Behavioral Theory in Privacy. "Protection motivation theory (PMT)," posits that an individual's motivation to protect themselves from a potential threat occurs through risk and benefit appraisals [77]. Risk appraisal assesses the perceived negativity of threat consequences (i.e., perceived severity) and the perceived likelihood of direct harm (i.e., perceived vulnerability) [91]. When perceived severity and susceptibility are high, protection motivation rises and an individual is prone to maladaptive behavior (e.g., denial or avoidance) [91]. Benefit appraisal (e.g., monetary rewards) may weaken protection motivation, particularly when the perceived benefit is higher than the perceived risk. In short, this cognitive process of weighing risks and benefits affects motivation and subsequent actions.

Originally discussed in the context of health threats, PMT has been diversified and applied to cybersecurity and privacy in recent years [38, 83]. For example, Workman et al's study [101] tested PMT to determine that people with adequate knowledge of a system fail to take security measures, showing the discrepancy between "knowing and doing." Another study in the context of online privacy explored the feasibility of PMT in explaining teenagers' willingness to disclose personal information on a website, which resulted in a higher willingness to provide information because of higher perceived benefits, albeit also highly perceived privacy risks [105].

Such human behavior can also be explained by the "privacy paradox," which refers to the human tendency toward privacy-compromising behavior, despite privacy concerns [67]. Although people express a strong desire to retain ownership and control of their data [58], they might not know how to take appropriate measures because of a lack of knowledge [108] on overall data practices (e.g., types of data being collected, collection purposes, shared entities, and data processing procedures) and potential misuse scenarios when collected long-term or combined with other data [63]. Some even attempted to sacrifice their privacy as they received financial gain or were burdened with data protection measures and relevant information [73].

In the light of these theoretical perspectives, we aimed to explore participants' perceived risks, benefits, and their behavioral intentions under the context of a large-scale sensor data collection project. In our study, we found that one's motivation to consent to data collection and its public release is affected by their perceived risks (i.e., privacy concerns) and perceived benefits (i.e., intrinsic/extrinsic motives). In terms of perceived benefits, we found two types of motives that drive participants' willingness to contribute to research: intrinsic and extrinsic. Intrinsic motives can be personal or social. Intrinsic motivations are values such as enjoyment and self-interest [46], while social intrinsic motivations are one's perceived contribution to community or community identification, which are defined as collective motives [13]. Extrinsic motives generally refer to monetary rewards [46], and many

previous studies in HCI research have shown a strong effect in motivating participants [53, 64, 76]. Despite these potential benefits, participants also expressed concerns about their personal data being collected and released. Thus, balancing risks and benefits is an important task for encouraging participants to contribute to a research project.

2.2.2 Privacy Concerns in Mobile Contexts. Considering the sensitive and personal nature of data collected from mobile and wearable sensors, ethical challenges especially centering on privacy concerns, should be addressed. Because of the passive and continuous sensing of these sensors, a vast amount of data that include biometric data (e.g., heart rate and gait patterns), behavioral data (e.g., mobility), contexts (e.g., GPS location and timestamps), and extra user data (e.g., self-reports) can be collected. This data stream enables personal profiling and behavioral predictions, which raises data privacy concerns of a participant and their consent to data collection.

Such concerns are well reflected in growing demands for ethical and regulatory considerations. For example, EU's General Data Protection Regulation (GDPR) [92] places a legal responsibility to protect participant data control and ownership. GDPR requires specific descriptions of collected data and its purposes, along with providing participants an option to consent on a granular level across the research lifecycle (e.g., consent (or not) separately to each new data collection in a longitudinal study). Along with GDPR, there's a growing discussion on MyData [8]. MyData is an emerging personal data management and processing vision that is specifically discussed in healthcare contexts. According to the notion, it allows a data subject to possess direct access, control and even ownership of the data and aims for user empowerment regarding their personal data, providing opportunities for users to be educated on how their data is used and by whom.

With rising concerns about data privacy, there has been an increasing interest in understanding user attitudes and privacy concerns in HCI studies. Earlier studies primarily focused on data collection from wearables and fitness trackers where researchers investigated user privacy concerns in sharing fitness data [9, 31, 75]. More recent studies have further explored privacy concerns in other domains such as mental health applications [74, 78] and personality detection system building [45].

The commonly reported results from these studies show that participants' comfort in collecting and sharing information depends on the type of information and their perceived risks and benefits [9, 65, 75]. Participants were generally generous toward collecting and sharing data derived from wearable devices (e.g., step counts, sleep) as they considered these types of data to be innocuous [31, 32]. As expected, participants were more concerned with sensitive and intimate data such as GPS, friends lists, photos, and social interactions [31].

While these studies have covered the ground in terms of understanding privacy concerns in sensor data, our study setup differs from previous studies in the following ways: 1) purpose and scope, 2) in-the-wild data collection, and 3) extensive range of collected data.

- *Purpose and scope*: Prior studies have primarily focused on privacy concerns in data sharing with popular application scenarios such as fitness tracking and location-based services. Our study focuses on exploring the motives and privacy concerns related to affective computing. We focus on a mobile and wearable sensor dataset collected in the wild which aims to facilitate the research and development of affective computing technologies. To the best of our knowledge, no prior studies have explored privacy concerns and associated factors for in-the-wild open dataset collection with mobile and wearable devices.
- *In-the-wild data collection*: Previous studies explored user privacy concerns mostly by relying on qualitative approaches with small-scale field trials or considering hypothetical scenarios [31, 74]. We conducted a relatively large-scale in-the-wild field study (N = 100) and discussed privacy concerns based on participants' everyday life experiences.
- *Extensive range of collected data*: Previous studies were confined to healthcare contexts and did not cover an extensive range of multimodal sensor datasets [9, 31, 75]. Our study aims to collect a broad range of

mobile and wearable sensor data as well as self-reports (i.e., psychological status data and ESM surveys) in the wild, which may contain sensitive and personal information about mental and affective states.

Considering the aforementioned background and current research gap, we explored the following RQs.

- RQ1: What are the participants' privacy concerns and general motives regarding in-the-wild open dataset collection for affective computing research?
- RQ2: What factors are associated with participants' attitudes toward the in-the-wild open dataset collection for affective computing research?

3 METHODS

We conducted a four-week open dataset collection project in-the-wild. We collected 31 data types from 100 university students (32 females, age: M = 22.82, SD = 3.28), through two different sources (i.e., smartphones and wearable devices). From the initial 109 participants, 9 of them were screened and excluded from further data analysis as they did not respond to our request to answer post-survey. As a result, we included only the data of a total of 100 participants.

Recruited participants were largely students from a large research-oriented university (N = 88) and other participants were students from nearby universities (N = 12). Majority of the participants were undergraduate students (N = 68). As to participants' majors, we observed diverse areas of scientific studies as the institution is devoted to scientific research. The top three majors were electrical engineering (N = 23), bioengineering (N = 17), and computer science (N = 12).

The study was approved by the university institutional review board (IRB). Our major goal in this study was to explore participants' attitudes and privacy concerns on mobile sensor open dataset collection for affective computing research. To deliver complementary insights, we took a mixed-method approach (i.e., survey and interview) and the study was designed across three phases: 1) before data collection, 2) during data collection, and 3) after data collection (see Table 1).

3.1 Phase 1: Before Data Collection

Before data collection, participants attended an off-line orientation and were informed of guidelines and the overall research process. As to the extensive range of data collection, we informed our participants that it is favorable to collect a large volume of data for developing high performance emotional intelligence algorithms (e.g., stress detection, mood inference). We also emphasized the importance and the necessity of contextual information (e.g., data types, sample instances) [2, 25] for in-situ context inference in the research, which inevitably collects a large volume of data across multiple sensor data.

3.1.1 Data Collection Information. At the orientation, we informed that the collected data will be publicly released after pseudonymization (i.e., removing all personally identifiable information). After the introduction, participants

Table 1. Types of data collected during each stage of the study

Before Data Collection	**During Data Collection**	**After Data Collection**
Survey (N = 100)	*Smartphone & Wearable sensor data* (N = 100)	*Survey* (N = 100)
– General survey (privacy)	– Physiological responses	– Data-sensitivity (post)
– Data-sensitivity (pre)	– User contexts	– Psychological status (post)
– Data release preference	– ESM survey	
– Psychological status (pre)		*Interview* (N = 26)

Table 2. Descriptions of collected data

Device	Category	Data Type	Description
Smartphone	Location	GPS	Location change (GPS signals)
	Network	Wi-Fi/Bluetooth/Cellular	Nearby wireless signals (e.g., SSID, SNR)
		Data traffic (Tx/Rx)	Network usage (Tx: transmitter, Rx: receiver)
	Device status	Power status	Power on/off, screen on/off
		Ringer mode	Normal/vibrate/silent
	Battery	Battery level	Charge state
		Charging status	Charging/discharging
	Calls/Text messages	Phone call history	Call history (with encrypted contact number)
		Text message history	SMS/MMS history (with encrypted contact number)
	Keyboard	Type of keyboard	Korean keyboard (chun-ji-in/qwerty/etc.)
		Type of input key	Character type (Korean/English/special/etc.)
		Distance b/w consecutive input keys	Grid length, time interval between input keys
	Media	Camera use / Screenshot	Type (picture/video), time of record
	App	App usage statistics	Installed app list, and app use history
		Notification history	App notifications at notification bar
	Activities	Types of activities	Physical activity (run/walk/in-vehicle/...)
	Psychological status	ESM survey	Mood status and duration, stress level, task attention level, disturbance level, mental load, and change of emotion
Wearables (Polar H10, Fitbit Inspire HR)	Biosignals	Heartrate	ECG signals (heartbeat)
	Activity types	Calorie	Daily calorie consumption
		Steps	Daily step counts
		Stairs	Daily number of steps climbed up
		Distance	Daily moved distance
		Sleep status	Sleep stage, sleep time

were asked to sign the IRB consent form and were informed of compensation (100,000 KRW, approximately $85), data protection measures that will be taken to protect participant privacy (e.g., data disposal upon withdrawal), and allowed to retract their consent (none of the participants did).

For participant privacy and transparency, we provided an additional document that offers detailed descriptions of each data sensing stream and what each device was capturing (see Table 2). Note that we informed our participants that we only collect meta-data and do not collect any content from call/text logs or photos during mobile data collection.

3.1.2 Data Collection Apparatus. Participants were informed to install a research team-made sensing app on their smartphones for mobile data collection and were also distributed with the Fitbit HR Inspire and Polar H10 devices (Fig. 1a). Since our sensing platform runs on Android phones with an operating system version 7.0.0 (Nougat) or higher, participants whose Android phones below this version were screened in the initial stage. Participants were allowed to check each collecting sensor in the configuration screen (Fig. 1b) on the platform and were asked to respond to ESM questionnaires during data collection (Fig. 1c). We elaborate on the ESM questionnaire in the following section.

3.1.3 Pre-Surveys. Participants were also asked to complete four survey questionnaires: 1) General survey, 2) Data-sensitivity survey, 3) Data release type preferences and 4) Psychological status.

1) General survey: For the general survey, we asked participants to rate their perceived level of agreement against each question based on a 7-point Likert scale (1: Highly Disagree ~ 7: Highly Agree, and N/A or don't know). Detailed question items are as follow:

- **Demographics**: Participants' age, gender, education
- **Confidence in knowledge**: Participants' self-assessed confidence and interest in their knowledge of the research context (e.g., mobile/wearable sensor data collection) and privacy issues.
- **Participation motive**: Participation motive for the research (i.e., financial compensation, interest in the research area, and contribution to scientific research).
- **Perception on open dataset collection**: Participants' general perception of open dataset collection for research purposes (negative or positive).
- **Risk-benefit assessment of open dataset collection**: Participants' attitudes toward perceived risks (e.g., privacy threats) and benefits (e.g., scientific contribution).
- **Perceived level of privacy concerns**: Participants' level of concerns toward perceived surveillance, perceived intrusion, secondary use of personal information, prior behavior experiences, and behavioral intentions in the context of mobile and wearable dataset collection and public release.
- **Level of trust**: Participants' assessment on their level of researchers and overall research process (e.g., data processing).

To design general privacy survey, most of the survey items were derived from prior studies in biomedical studies [66, 68, 82], as the field has long studied participants' willingness to participate and contribute to data collection due to its constant collection of personally sensitive data (e.g., health records, genetic data). As to privacy concerns and trust, we referred to a widely-used scale from the field of information science [57, 102, 103] (see Table 3).

Each survey item was contextualized to reflect our research setting. We also went through several iterations of the survey items and overall structure and conducted pilot tests with five participants to identify participant concerns, verify the appropriateness of wording, and test completion time.

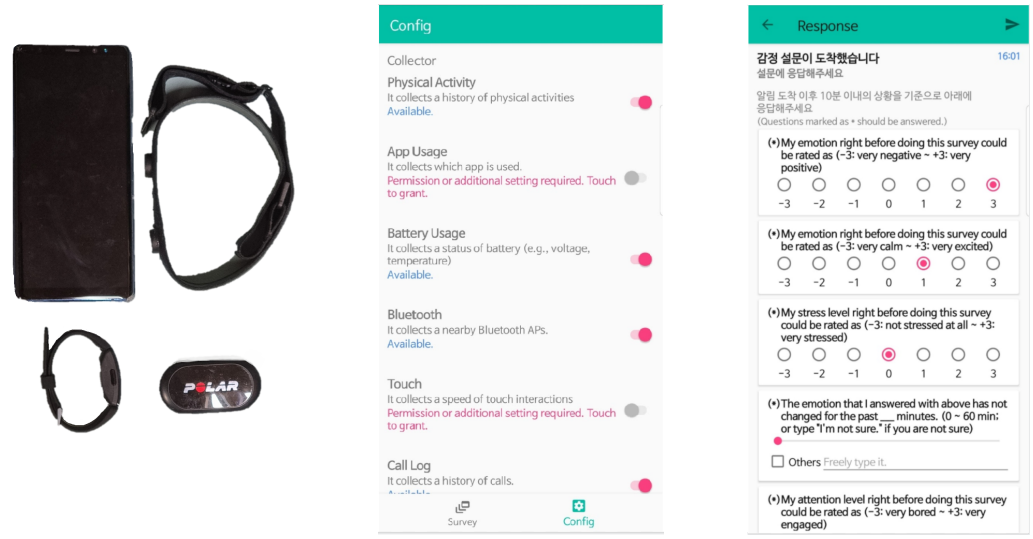
2) Data-sensitivity survey: Participants were also asked to rate their *perceived sensitivity* of each collected data. We asked participants to rate their comfort level in publicly releasing each data stream, which was also a 7-point Likert scale (1: Highly Negative ~ 7: Highly Positive, and N/A or don't know). We designed this survey because we assumed that people's comfort levels and types of concerns differ by the information types and one's awareness of potential issues in privacy [3].

3) Data release type preferences: After reviewing the given document that offered data collection information, we provided participants an option to choose their preferences for data release. This was conducted to grasp the initial overview of participants' attitudes on data release and to elicit sharper views on privacy later in the interview. The two given options were *complete release* and *selective release*. Participants who felt comfortable in releasing all of their data signed up for complete release, while participants who perceived certain data types to be privacy-sensitive signed up for selective release. For the latter, participants were asked to select data types they wished to exclude via Google Form link. Note that participants were not allowed to change their data sharing configurations (e.g., unshare certain data types) during the study period.

4) Psychological status: Self-report questionnaires were given to classify participants' psychological characteristics. We used PSS [20] to measure the level of perceived stress during the data collection period. We also measured mental health with GHQ-12 [59] and PHQ-9 [47], and personality traits with BFI-K-15 [44]. In addition, we collected positive psychological capital (PPC) [55], self-esteem (RSE) [52], life satisfaction (SWLS) [56], and overall class satisfaction. Since analyzing all the results from these questionnaires is not the scope of this work, we do not report them in detail.

3.2 Phase 2: During Data Collection

During four weeks of data collection, participants were asked to answer Experience Sampling Method (ESM) questionnaires (Fig. 1c), which is widely used tool to capture people's in-situ experiences (e.g., behaviors,



(a) Smartphone and wearables (b) Configuration screen (c) ESM questionnaire screen

Fig. 1. Data collection apparatus and screenshots of sensing platform

Table 3. Reference lists of each survey item from the general survey

Survey Item	**Reference**
Demographics	-
Confidence and interest in knowledge	-
Participation motive	-
Perception on open dataset collection	Shah et al. 2019 [82]
Risk-benefit assessment of open dataset collection	Oliver et al. 2012 [68], Shah et al. 2019 [82]
Perceived level of privacy concerns	Xu et al. 2008 [102], Xu et al. 2012 [103]
Level of trust	Liu et al. 2005 [57]

thoughts) [50]. Participants were asked to report their psychological states, such as mood, stress level, attention level, mood duration, disturbance level, mental load, and emotion changes. The questionnaires were given at least 10 requests per day, which is similar with the average number of daily requests in prior ESM studies (M = 12.3, SD = 4.4, range= 8 ~ 20) [28, 36, 61, 81, 97, 100].

3.3 Phase 3: After Data Collection

3.3.1 Post Data-Sensitivity Survey. After four weeks of in-the-wild data collection, we conducted a post-survey on 1) data-sensitivity and 2) psychological status. Particularly, post-survey on data-sensitivity was essential for us because we wanted to see whether participants' perceived sensitivity would be affected after actual in-the-wild data collection.

3.3.2 Interview. To understand users' perspectives and determinants that affect their attitudes in the public release of the mobile/wearable dataset, we conducted semi-structured interviews with 26 participants in person,

each lasting 30-40 minutes. Out of 26 interviewees, 15 participants were from those who made a selective release choice. For the other 11 participants, we randomly selected interviewees from those who made a complete release choice. We recruited interviewees from both groups to compare whether participants perceive their data privacy differently depending on their choice. All interviews were structured around a predetermined set of questions designed to cover a wide range of data release and privacy-related topics.

The goal of our interview was to identify factors that affect participants' attitudes toward the open dataset collection. The interview protocol had three major components. First, during the interview, participants were presented with the lists of collected data in the research and asked to freely discuss their opinion on open dataset collection for research purposes. We also asked them about the types of factors that affected their attitudes. Second, we asked their opinions on collecting diverse streams of data from various sources (i.e., smartphones and wearable devices) and the types of privacy concerns they had during data collection. Third, we asked selective release participants whether they're willing to convert to complete release if given an option to be paid additional compensation (10,000KRW, approximiately $8).

Once interviews were complete, we conducted a thematic analysis. Thematic analysis is a widely used qualitative research method to identify salient patterns or themes in the data [17]. For theme searching, we went through the following 6 phases: familiarization with the data, generating codes, searching for themes, reviewing themes, defining and naming themes, and producing the report. Following the approach, we performed the analysis in a bottom-up, iterative fashion.

4 RESULTS

We first provide descriptive data to provide the necessary backdrop for interpreting the qualitative results that follow. Then we describe interesting findings from our qualitative data analysis.

4.1 General Motives and Privacy Concerns (RQ1)

For RQ1, we report our findings from general survey and data sensitivity survey (pre-post). With these results, we aim to answer the following sub-questions with a specific focus on privacy:

- RQ1-1: What are the participants' perceived level of privacy concerns and general motives regarding open dataset collection?
- RQ1-2: How does the participants' perceived sensitivity differ across different data types?

4.1.1 RQ1-1: Privacy Concerns and General Motives. To answer this question, we report our findings from the general survey conducted before data collection. We consider this exploration to be meaningful, since we provide thorough participant perspectives on mobile sensor open dataset collection. According to a study on information sensitivity and disclosure [62], it says exploration on factors such as perceived risks and benefits are measured as an antecedent for willingness to disclose items of personal data. Likewise, our general survey intends to provide overall information that is necessary for understanding participants' sensitivity and attitudes toward the collection and release of the data.

Descriptive summary of survey results: Here, we report some interesting findings from our survey (see Table 4). Revisiting our method, we asked participants to rate their perceived level of agreement on each given question (1: Highly Disagree ∼ 7: Highly Agree, and N/A or don't know). As to *motives*, financial compensation was shown as the most influential participation motive (M = 5.67, SD = 1.20), and 87% of responses ranged from scale 5 to 7. Following were scientific contributions (M = 4.32, SD = 1.43), interests in AI service-related research (M = 3.89, SD = 1.72), and interest in data collection (M = 3.73 , SD = 1.64).

In assessing *perceptions* on mobile sensor open dataset collection, we asked participants to rate two different questions: whether their data being released 1) without his/her own data (i.e., general sense), or 2) with his/her own data (i.e., personal sense). We designed these two conditions based on pilot study feedback, which reported

Table 4. The descriptive statistics of general survey results
(1: Highly Disagree ~ 7: Highly Agree, and N/A or don't know)

Category	Survey Item	Mean	SD
Confidence in knowledge	Self assessed knowledge on mobile/wearable devices	4.13	1.68
	Self assessed knowledge on sensor data research	3.51	1.55
	Self assessed knowledge on personal data protection	4.25	1.37
Motives	Interest in data collection	3.72	1.64
	Interest in AI service	3.89	1.73
	Financial compensation	5.67	1.20
	Scientific contribution	4.32	1.43
Perception	With my data	5.05	1.33
	Without my data	4.85	1.45
Risk-benefit assessment	Perceived importance of scientific contribution	4.12	1.39
	Perceived importance of personal data protection	6.40	1.02
	Perceived importance of potential benefits in this research	4.68	1.51
	Perceived importance of potential risks in this research	3.70	1.45
Privacy concerns	Perceived surveillance	4.01	0.04
	Perceived intrusion	4.29	1.52
	Secondary use of personal data	4.50	0.04
	Behavioral intention	5.15	1.53
Trust	Trust in collected data types	6.16	1.09
	Trust in data collection purpose	6.07	1.13
	Trust in potential usage of collected data	5.82	1.22
	Trust in data not being shared with third-parties	5.70	1.49
	Trust in data not being shared without permission	5.94	1.15
	Trust in the necessity of collected data	5.78	1.14
	Trust in the overall process	5.25	1.61

concerns on potential misleading results depending on a reference point (themselves vs. in a general sense). Our results showed participants outweighed the importance of data public release with his/her data (M = 5.05, SD = 1.33) over that without his/her own data (M = 4.85, SD = 1.45), which we posit such tendency is due to potential privacy concerns.

In terms of *risks and benefits*, we also asked participants to answer two different dimensions: general sense vs. personal sense. Here, note that we report the average value of means as there were no significant differences among two different dimensions. In interpreting the results, we spotted an interesting mixed response of participants. In terms of importance of personal data protection and scientific contribution, participants outweighed the importance of personal data protection (M = 6.41, SD = 1.04) over scientific contribution (M = 4.12, SD = 1.39). However, in their assessment on the importance of general benefits and risks of open dataset collection, participants highly assessed potential benefits (M = 4.68, SD = 1.51) greater than potential risks (M = 3.70, SD = 1.45). This is interesting to note since participants reported low concerns on potential risks although they were aware of the importance of personal data protection.

With regard to overall *privacy concerns*, participants showed a moderate level of concerns. Participants were primarily concerned with potential secondary use of personal data (M = 4.50, SD = 0.04), which includes scenarios such as personal data being released without notification or authorization, or released with unknown entities for other purposes. More than 40% of the participants perceived themselves as being the subject of surveillance (M = 4.01, SD = 0.04). Perceived surveillance covered participants' reported level of potential surveillance, collection, and sharing of personal data via smartphones and wearable devices. Participants also showed a moderate level of concern in perceived intrusion (M = 4.29, SD = 1.52), which reflected participants' concerns on personal data being readily available to unknowns without their acknowledgement and their perceived level of uncomfortable feelings in using smartphones and wearable devices. In terms of behavioral intentions, participants were willing to participate in similar future research (M = 5.15, SD = 1.53). As to questions on prior experiences related to privacy, more than 60% of the participants reported having no such experiences or no knowledge.

Participants' overall responses on their level of *trust* toward the research process and researchers were higher than the other question items (M = 5.82, SD = 1.26). Upon closer inspection, we see that participants showed a relatively higher level of trust in collected data types and its purpose. In terms of overall trust in the research process, participants showed the lowest level of trust.

4.1.2 RQ1-2: Data Sensitivity and Privacy Concerns. To further understand the participants' acceptability and concerns in collecting vast amounts of sensor data, we collected another 7-point Likert scale survey (1: Highly Negative ~ 7: Highly Positive, and N/A or don't know). We asked participants' perceived sensitivity of each data type *before* data collection and *after* data collection.

Table 5 and Table 6 show the participants' reported sensitivity before and after data collection. Here, note that *the lower reported value indicates higher sensitivity*. We found that participants responded sensitive to certain data types from smartphones, while they showed generally moderate levels of sensitivity toward other types of data from wearables and self-reports.

Representative data types that reported high level of sensitivity were *text logs*, *call logs*, *app usage*, *app notifications*, *camera* and *GPS*, which were indicative of one's personal life or social boundaries. We found that the order of these data did not change significantly after data collection.

Comparative analyses: To explore whether actual in-the-wild sensing and data collection experience affect participants' sensitivity, we statistically compared participants' data sensitivity. We used two-way Mixed-ANOVA with the temporal difference (pre vs. post) and release options (selective vs. complete) as independent variables and data sensitivity score as a dependent variable. Our results showed no significance for the main effects (temporal difference: ($F_{1,97}$ = 1.17 , p = .56, η^2 = .006); group difference: ($F_{1,97}$ = .53 , p = .47, η^2 = .005). In addition, the interaction effect between the main effects was also not significant ($F_{1,97}$ = 1.17 , p = .28, η^2 = .012). These results suggest that data sensitivity scores do not vary across release options, and did not change after the experience.

Selective release choice: Table 7 reports results specific to participants who opted for selective release (N = 15). Given an option to select specific data types they wished for *non-release*, the most frequently selected non-release data types were GPS and app usage (N = 8). Followed were app notifications (N = 7), texts (N = 4), calls, camera, type of input characters, key distance (N = 3), and WiFi, data bytes, activity types (N = 1). As to wearables and self-report data, one participant selected heart-rate, PSS (perceived stress), PHQ-9 (depression symptom), RSE (self-esteem), SWLS (life satisfaction) and class satisfaction.

In terms of data sensitivity, representative data types that reported high level of sensitivity were *text logs*, *app usage*, *call logs*, *GPS*, and *camera*, which showed similar results from our previous analysis from total participants.

4.2 Factors Associated with People's Attitudes on Open Dataset Collection (RQ2)

In this subsection, we answer RQ2, "What factors are associated with participants' attitudes toward the in-the-wild open dataset collection for affective computing research?" As noted, we conducted semi-structured interviews on

Table 5. Pre-post sensitivity of each sensor data
(1: Highly Negative ~ 7: Highly Positive, and N/A or don't know)

Device	Category	Data Type	Pre-Sensitivity		Post-Sensitivity	
			Mean	SD	Mean	SD
Smartphone	Location	GPS	3.89	1.54	3.72	1.60
	Network	Wi-Fi/Bluetooth/Cellular	4.15	1.45	4.14	1.52
		Data traffic (Tx/Rx)	4.36	1.62	4.34	1.59
	Device status	Power status	4.58	1.46	4.62	1.52
		Ringer mode	4.38	1.43	4.21	1.50
	Battery	Battery level	4.86	1.31	4.97	1.35
		Charging status	4.89	1.31	4.93	1.29
	Calls/Text messages	Phone call history	3.33	1.58	3.17	1.53
		Text message history	3.29	1.62	3.11	1.58
	Keyboard	Type of keyboard	4.68	1.64	4.81	1.64
		Type of input key	4.40	1.68	4.41	1.68
		Distance b/w consecutive input keys	4.20	1.77	4.28	1.80
	Media	Camera use event	3.88	1.55	3.76	1.60
	App	App usage statistics	3.41	1.71	3.18	1.65
		Notification history	3.70	1.54	3.45	1.59
	Activities	Type of activities	4.85	1.40	4.92	1.53
	Psychological status	ESM survey	4.45	1.51	4.30	1.52
Wearables (Polar H10, Fitbit Inspire HR)	Biosignals	Heartrate	4.78	1.51	4.82	1.62
	Activity types	Calorie	4.88	1.46	4.98	1.41
		Steps	4.79	1.41	5.11	1.48
		Stairs	4.89	1.45	5.04	1.50
		Distance	4.78	1.40	4.85	1.54
		Sleep status	4.69	1.50	4.30	1.52

Table 6. Pre-post sensitivity of psychological status data
(1: Highly Negative ~ 7: Highly Positive, and N/A or don't know)

Data Type	Pre-Sensitivity		Post-Sensitivity	
	Mean	SD	Mean	SD
PSS	4.42	1.51	4.35	1.49
GHQ-12	4.58	1.54	4.67	1.52
PHQ-9	4.24	1.60	4.34	1.58
BFI-K-15	4.21	1.63	4.25	1.64
PPC	4.43	1.49	4.43	1.51
RSE	4.32	1.54	4.35	1.59
SWLS	4.41	1.55	4.37	1.57
Class satisfaction	4.59	1.52	4.59	1.51

26 participants (P1 - P15: selective release, P16 - P26: complete release) after four weeks of data collection. To answer this question, we report our results from the thematic analysis presented in Table 8. We have selected

Table 7. Non-release data types and responses to additional incentive offer: Before data collection, participants from selective release choice were asked to choose data types they wished to exclude (i.e., non-release data). After data collection, these participants were asked if they are willing to convert to complete release at the expense of being paid an additional incentive.

Participants	Non-Release Data	Incentive Offer
P1	Type of input key, Distance b/w consecutive input keys, Camera use events, App usage statistics, Notification history	
P2	Distance b/w consecutive input keys, App usage statistics, Notification history	
P3	GPS, Phone call history, Text message history, Type of input key, Camera use events, App usage statistics, Notification history	
P4	Notification history	Yes
P5	Distance b/w consecutive input keys, App usage statistics	
P6	GPS, Phone call history, Text message history, Type of input key, Camera use events, App usage statistics, Notification history, Heartrate, PSS, PHQ-9, PPC, RSE, Class satisfaction	
P7	GPS, Phone call history, Text message history, App usage statistics, Notification history	
P8	Notification history	
P9	GPS	
P10	GPS	
P11	Notification history	
P12	GPS, Phone call history, Notification history	Yes
P13	GPS	
P14	GPS	
P15	GPS	Yes

the most interesting or salient quotes and anecdotes to embody each theme; these examples are meant to be illustrative but not exhaustive.

4.2.1 Incentives. Financial incentive was frequently cited as an influential driving factor that affects participants' views on open dataset collection. Interestingly, participants showed contradicting responses toward two types of factors that affected their attitudes. Here, we categorize these two factors.

Participation compensation: Overall, participants perceived participation compensation as a significant benefit. P3 stated, "*Of course I did it for the money! (laughs) Money was the number one reason, but later on, I also came to think about the scientific contribution that I can make from agreeing to this open dataset collection.*"

Privacy-utility trade-offs: Upon our offer of additional incentive given at the expense of converting to complete release, participants with selective release showed mixed responses. The responses showed varying degrees of disagreement. For example, P6 reported, "*Only 10,000 KRW [approximately 10 USD] for complete release? Come on, you guys are being cheapskates! I'd reconsider if the offer was higher.*" Although most participants from selective release refused the offer, three participants were willing to convert to complete release. Some participants would reconsider the value of their data at the expense of their privacy [37]. For example, P14 said, "*I only selected GPS. Now that I think about it, my life is so routine that my data would look nothing special. I think I'd be okay!*"

4.2.2 Knowledge and Experience. Some participants were drawn to the knowledge and experiences that this research could offer.

Research interest: Some participants showed great interest in the overall process of our large-scale data collection research. P17 noted, "*I got interested in personal data collection after taking statistics class, because I had to collect my data for the assignment. I wanted to see how a real experiment collects this massive amount of data from such many participants.*"

Learning personal life patterns: Participants' interest in self-tracking through wearable devices and attempts to learn his or her life patterns positively influenced their thoughts on open dataset collection. P25 reported,

Table 8. Factors associated with participant's attitudes on in-the-wild open dataset collection for affective computing research

Theme	Sub-theme	Description
Incentive	Participation compensation	Financial compensation given upon the participation
	Privacy-utility trade-offs	Additional incentive offered upon conversion to complete release
Knowledge and experience	Research interest	Interest in the data collection experiment (e.g., AI service, Data analysis methodology)
	Learning personal life patterns	An attempt to gain an insight on one's life pattern (e.g., exercise routine, sleep patterns)
	Wearable device experience	Wish to have a wearable device experience
Scientific contribution	Data volume	A motive to contribute to the wealth of data volume
	AI service / Related research	A motive to contribute to research development
	Institutional scientific contribution	A motive to contribute to development of the research institution
Privacy risks	Routine identification	A sense of discomfort incurred by potential inference of someone based upon one's routine data
	Judgment/Categorization	A sense of discomfort incurred by a potential judgment on an individual's personal trait inferred from the data
	Surveillance	Fear of being monitored
	Data misuse/leakage	Fear of data misuse and leakage to other unknown third parties
Lack of justification	Research purpose	Lack of understanding on the research context and purpose
	Sensor data usage	Lack of knowledge on potential usage of the collected sensor data
Degree of perceived autonomy	Higher autonomy	High level of perceived autonomy due to given option to choose data disclosure
	Lower autonomy	Low level of perceived autonomy due to a sense of helplessness
Trust	Institutional trust	High level of trust owing to the institution reputation
	Data handling trust	Low level of trust in data processing

"*I'm interested in measuring how much I exercise and move around each day. Oh, by the way, I signed up for this experiment with my friend. Since we get to wear the same wearable device for a month, we thought it was a good opportunity to compare our time and amount of workouts.*"

Wearable device experience: Desire to experience wearable devices was another cited reason. P19 said, "*I've always wanted to wear smartwatches and track my activities. I think I wore Fitbit literally 24 hours!*"

4.2.3 Scientific Contribution. Altruistic motives such as contributing one's data toward scientific research were also highlighted as one of the key factors. Several participants saw the potential societal benefits of open dataset collection. Some participants also expressed enthusiasm and hope about the vision of emotional intelligence research. Here, we categorize the types of scientific contributions commonly mentioned during the interview.

Data volume: Participants expressed positive attitudes as they felt they were donating their data. Some of them were aware of the necessity of the large data amount required for machine learning. For example, P8 noted, "*For research like this, you need a large amount of data for analysis and better outcomes. The more, the better! I know this because I'm doing similar research. So I feel you guys.*"

AI service and related research: Contribution to relevant AI services and other similar research that leverages collected data was also a critical factor. Participants outweighed potential benefits for the public good rather than individual benefits (e.g., financial compensation) or potential risks (e.g., privacy concerns). P20 reported, "*I remember you said the data will be used for AI services that infer emotions? Well, I think such values are important. I don't care about the money. Money doesn't last, but research contribution and development do. You never know!*

Maybe the data from this research will eventually benefit many people in general and I'd be proud to say I was part of this process."

Institutional scientific contribution: Several participants saw potential in how an open dataset collection would benefit the reputation and advancement of the research institution. Some participants identified themselves with the researchers, as they were graduate students. They expressed a sense of community and affection toward the research institution. For example, P7 noted, "*Umm, I think this experiment could be a bit dangerous as it collects and aims to release an extensive dataset of an individual. However, I do this because this institution is dedicated to scientific research and I'm also a member of the community. I wouldn't have made the same decision if it was for another institution.*"

4.2.4 Privacy Risks. Unlike aforementioned positive attitudes, participants were doubtful in consenting to open dataset collection due to concerns about privacy risks they experienced during the data collection. As supported by our data sensitivity survey results, participants from the selective release group expressed more concerns about privacy risks. Reported sources of privacy risks varied due to various factors such as the scope and nature of the data, social desirability, control over data collection, and potential misuse of the data. We situate the sources of privacy risks as follows.

Routine identification: Participants expressed uncomfortable feelings toward their routine data being revealed and identified. As one's routine data potentially entails one's personal life and whereabouts, they were pessimistic about the open dataset collection. For example, P9 noted, "*I visit my girlfriend's house once or twice a week. Then someone might take a look at my data and think, 'Oh, this guy always drops by this spot at this time of the week? What is this place?'*" P9's concerns were exacerbated as he imagined the most privacy-sensitive scenario by combining other data types. "*And if you combine this location data with my heart rate or sleep patterns around that time and if my heart rate skyrockets, you may wonder what I'm doing! I know this is a bit exaggerating and people won't even care. But still, it's embarrassing and it matters because I know what the data means. That's why I said no to my GPS release.*"

Judgment and categorization: Unwanted judgment or categorization of an individual based on one's data also raised concerns on privacy risks. Some participants showed more serious concerns than we expected. Despite knowing that the data was being pseudo-anonymized, some participants expressed concerns about being reviewed and judged by researchers and the public. P7 expressed concerns about being stigmatized as a *loner*, "*I didn't want my call/text logs to be released ironically because there's nothing… I only have a few friends and only a handful of contacts… So people would naturally assume that I'm a loner and anti-social. Even though you told me that the data are anonymized, I just hate it.*" In addition to this categorization, one participant expressed further concerns on the possible re-identification. For example, P6 reported a high level of concern about his identity being directly revealed by his close friends within the school. P6, the only participant who selected self-report data types (i.e., psychological status and ESM surveys) that are related to stress, perceived self-esteem, and depression, also reported his concerns, saying "*I have some symptoms of depression... I just don't like the idea of people figuring it out and saying, 'Oh, this one is a depressive one.' What if the data is released within our school for similar research projects? People may not know, but I'm sure someone close to me would notice!*" Such response is interesting to note, as other participants were concerned about being labeled as a certain type of person (e.g., loner) rather than their identity directly being revealed.

Surveillance: Fear of being monitored arising from certain data types was also reported from participants. Participants expressed sensitive responses toward their content data (e.g., call/text messages) being monitored. Although we showed detailed terms of use - including specific data types being collected and high-level individual summary of such data - and informed that their content data will not be collected nor encrypted, this still gave users room for imagination on collected data usage. Particularly, for key distance, we informed participants through IRB and additional document that we do not collect the raw keystroke data and will not attempt to

reverse-engineer the original input keys from the data we collect. However, P11 said, "*You see, I feel kind of upset and also scared. For example, the app notification data would probably show pop-ups of personal messages and notifications I received from each app that I use. I feel being monitored. Also, I was upset with the key distance data. If I'm right, key distance equates with text message contents if you do the math. Then, don't you think it's easy to infer my personal life?*"

Data misuse and leakage: With regards to concerns that participants have about potential data misuse and leakage, it was relatively less reported compared to other sources of privacy risks. P5 showed concerns on inadvertent data leakage, reflecting on his own experience, "*I've done similar research and once a data of a participant was leaked by mistake. Thank god it wasn't very personal data, but still, things like that can happen!*" Although P1 showed an optimistic view about the overall research ethos, he feared potential privacy threats. "*I know that this is a very low chance, but there could be some malicious actors and hackers. You never know.*"

4.2.5 Lack of Justification. Clear justification for the research purpose and data collection is an important prerequisite for participants' agreements on an open dataset practice, but several participants pointed out the lack of justification in research purpose and sensor data usage has made them hesitant in agreeing to open dataset collection.

Research purpose: Although we informed detailed information of our research purpose and the need for data collection, participants reported that the given information was not sufficient. Due to a month-long data collection, most participants forgot the types of data collected and other research-related information. P2 reported, "*I remember you giving explanations in the orientation, but I don't remember since there is too much data collected and it's been so long. I couldn't tell why this massive data collection was necessary for this research.*"

Sensor data usage: Participants also lacked understanding of what each data was trying to capture or why the data was necessary for our research. Some participants were doubtful and even showed negative responses toward certain data types and their usage. Participants pointed out that the given information is limited (e.g., insufficient information on raw data with an appropriate explanation of its use), suggesting that the information is too abstract and needs further specification. We posit that the extensive range of data and lack of background knowledge may have affected such insufficient understanding of the data usage. P10 stated, "*I'm not sure to what extent this is possible, but I think you can infer someone's passwords with key distance and keyboard data. Why do you need this data for emotional intelligence research? The paper you gave us earlier just lists the types and descriptions of the data, but it doesn't tell us why you need that specific data and how you're going to use it for the analysis. It's kind of hard to associate some data with emotion-related research.*"

4.2.6 Degree of Perceived Autonomy. Participants reported mixed responses in terms of their perceived autonomy. Participants who believed they were granted high or full autonomy responded positively to open dataset collection, whereas those who perceived lower autonomy showed negative responses and concerns.

Higher autonomy: Most of the participants who perceived higher autonomy were from the complete release choice. They appreciated an option to choose data release type (i.e., complete release vs. selective release) and reported such option that grants user autonomy led them to choose complete release. P21 stated, "*Anyway, I signed up for this data collection experiment at the expense of financial compensation. So I thought I had no right to my data. But the offer to choose the data release type made me trust the researchers and also think that I have the right to my data. Ironically this brought me some sort of relief and I figured complete release would be just fine.*"

Lower autonomy: Participants who perceived a lower level of autonomy showed skeptical and even defeatist attitudes toward their autonomy. For example, P6 reported, "*I signed up for this experiment, so technically I don't think I have the right to my data. The documents that you handed us earlier… Honestly, I think those are just token measures to show that this research is safe and privacy-protective. I chose selective release and I think this is the least I can do to protect my privacy.*"

4.2.7 Trust. "Trust" was also an often-cited keyword during the interview. Although participants generally showed a high level of trust toward researchers and research institution, participants expressed mixed responses in data handling processing. Participants' response to the relatively lower level of trust in the data handling process is also reflected in our general survey results.

Institutional trust: The majority of participants expressed an overwhelmingly positive response to the research institution, as the institution is dedicated to scientific research. P17 reported, "*I trust the reputation of the school and the experiment will eventually help scientific research in Korea.*"

Data handling trust: Participants were concerned about potential errors that can occur during the data processing. P3 stated, "*I trust the researchers but there's always human error. There could be some technical issues in the server or decryption process... So, I can't trust the research 100%.*"

5 DISCUSSION

We summarize the major findings by discussing data sensitivity and privacy concerns, and encouraging data contributors' motivations. In addition, we present the design implications for enabling context-aware privacy support for mobile open dataset collection.

5.1 Data Sensitivity and Privacy Concerns

5.1.1 Privacy Concerns: Data Types vs. Combination. Although participants generally reported low levels of privacy concerns, we were able to extract meaningful insights from their reported concerns regarding specific sensor data types. Note that these detailed interpretations are mainly observed in the interview responses of the participants with a selective release choice. The results of our survey and interview concretely inform the user-centric perceived sensitivity in each sensor data and other types of data being publicly released for research purposes.

Smartphone sensor data: In assessing data sensitivity, participants appeared to have relatively higher sensitivity in the following order: *text logs*, *call logs*, *app usage*, *app notifications*, *camera*, and *GPS*. These data types were also ranked (top six items), and there was only a slight difference in the sensitivity. Our participants expressed concerns because these data types could serve as potential indicators of personal traits and social behaviors. This finding is not surprising in light of recent studies that showed that call, text, and app usage are potent indicators of one's personality traits [23, 79].

Our analysis revealed that participants' primary concerns were centered on potential judgment/categorization and ubiquitous surveillance. Participants commonly reported discomfort from being monitored and judged based on their data (e.g., data from less social persons). This finding appears to be contradictory because the participants clearly understood that the collected data would be pseudo-anonymized for public release. Therefore, we expected that the participants would not report high levels of sensitivity. We asked them to explain why they had such sensitivity despite their awareness of data processing. Our participants deemed their gut feelings toward sensor data (e.g., discomfort) and expressed uncomfortable feelings toward the researchers' reviewing their data. They also reported a lack of trust in the research team in terms of the end-to-end procedure for data processing and handling. Such responses align with a previous study [73], which suggests that a wide scope of data collection raises *intuitive concerns* (associated with a fast and automatic thinking process) among participants even though they were notified of the purpose and scope of data collection by researchers.

Wearable sensor data and psychological status data: In terms of wearable devices (i.e., Fitbit Inspire HR, and Polar H10) and psychological status data that were given prior to data collection, participants reported relatively low levels of sensitivity and privacy concerns. This indicates that the participants predominantly perceived that their smartphones entail more privacy risks compared to other devices. Overall, participants

perceived data from wearable devices to be innocuous and found it difficult to associate their potential usage (e.g., sleep, step counts) in affective computing research.

Data combination: When multiple data types are combined, however, our participants expressed concerns that data combination (e.g., sensor data and ESM survey & psychological status data) would reveal or pattern their privacy-sensitive contexts and perceive that potential privacy risks would be leaked from the combination. Our participants self-assessed their risks by hypothetically combining multiple types of sensor data across different sources (via what-if analyses). This finding is consistent with prior study results that privacy concerns regarding seemingly benign data (e.g., step counts) may increase over time when combined with different social contexts [32]. Statistical learning offers advanced methods of combining multiple data types (e.g., accelerometer with GPS or WiFi data) to induce more finely specified and context-specific behaviors (e.g., the degree of physical activity in different locations) [34, 98].

5.1.2 Reasons for Weak Privacy Concerns. Although the selective-release group showed a higher level of privacy concerns and data sensitivity, we found that most participants were largely carefree with potential privacy risks in participating in open dataset collection. There are several explanations for the weak privacy concerns:

Perceived risks and benefits: Viewing participants' behavioral intentions through the lens of PMT [77], we find that privacy concerns serve as *perceived risks*, prompting participants to reconsider their decision in data collection and public release. As to *perceived benefits*, we find both (1) financial compensation and additional incentives (i.e., extrinsic motives) and (2) a sense of altruism (i.e., intrinsic motives). Although several sensitive privacy concerns were perceived as potential risks, our study found that participants also appreciated the importance of benefits this research offers, contributing to shaping participants' motivations in complying with data collection and public release.

In terms of financial motives, our results confirm the well-known effects of previous privacy studies; i.e., people are willing to accept personal benefits or discounts in exchange for their personal data [5, 37, 84]. Indeed, three participants who belonged to the selective release choice were willing to convert their decision to complete release for additional financial incentives. We posit that the immediate, tangible benefits of agreeing to data collection and public release are perceived greater than the costs (e.g., privacy risks) of doing so, which are uncertain and incurred at a more distant point in time [5].

This finding is somewhat different from prior crowdsensing research, in which micropayments were used to motivate participants [41, 76, 106]. We hypothesize that mobile sensor open dataset collection requires continuous collection and release of a large amount of personal data, and which significantly increases a user's level of expectations about financial compensation. One potential application of micropayments would be to increase behavioral compliance during data collection, by offering additional incentives to users on top of the baseline payment.

We also show that participants were drawn to altruistic motives "for the greater good." Aside from financial motives, contributions to scientific research were also deemed important across participants, both in surveys and interviews. Some participants strongly expressed pure interests and intentions to contribute to research over financial motives. Such results call for the HCI community to think more about our own responsibilities, especially in terms of encouraging altruistic behavior for the research development and overall public good.

Control paradox: When asked to choose data release preferences, only 15 out of 100 participants opted for selective release, which offers an additional layer of support to this finding. One plausible explanation to such a low number of selection may be because of the "control paradox," which refers to an illusory concept that people conceive [16]. According to this concept, people underestimate their level of risk owing to their misconceptions in data control, and are more likely to share personal data. Such tendencies can also be noted in our interview results. Several participants reported higher levels of autonomy due to a given option to choose data release

preference which ironically led them to select complete release, thinking they had greater control in their data than they expected.

Lack of privacy mental model: Our comparative analysis of data sensitivity (pre vs. post) showed no statistical significance. We posit a weak mental model for each sensor data and its associated usage with the research context may have affected the results. While we re-reviewed the document that provided a list of detailed descriptions of each data sensing stream and what each device was capturing, we observed that the interview participants' level of knowledge about data collection was quite limited or that they had some misunderstandings. Participants were largely unaware or unsure of what data was being collected, what each data meant for, and how it would be used. Although participants with selective release choice were shown to have a higher level of contextual knowledge and specific sensor data, they still lacked understanding of the research and collected data. Some participants were even more perplexed by the combination of diverse data types, which made it difficult to envision all the potential harms. We posit that such limitations may have created "bounded rationality" of participants[4], which may have hindered them from systematically evaluating actual risks .

5.2 Context-Aware Privacy Support for Mobile Open Dataset Collection

Mobile open dataset collection is largely based on traditional informed consent models where participants are given one-time instruction and their informed consent is obtained at the beginning of a study. However, we found that such traditional informed consent models for mobile sensor open dataset collection were limited because participants showed bounded rationality in making decisions. Mobile open dataset collection naturally assumes that we collect a large amount of contextual information; this dataset per se can be leveraged to enable privacy-by-design for mobile open dataset collection with context-aware privacy support.

5.2.1 Informing and Browsing. Although the participants were given an informed consent document that entailed a high-level description of each sensing stream, they would rarely read the document in detail and lacked knowledge of the collected data. Such findings suggest the need for a system design that helps users inform how their data are used and by whom, by providing the education related to data collection and use [11]. Offering such participant-centered design choices will increase participants' awareness of data collection and release, thus leading to their more proactive engagement in research. One possible design approach is to guide participants' choices through delivering privacy notices [27, 40]. For example, we can envision a system that assesses relevant privacy risks with visual guidance (e.g., visualizing data flow) [11]. Designing personalized privacy nudge interventions that regularly alert participants about sensitive data collection and offer an option to browse their data is also worth considering [7, 72]. Furthermore, we can proactively educate the participants by introducing context-aware intelligent agents such as chatbots. Intelligent agents can analyze the overall data contribution practices (e.g., types of data collected under specific contexts, trade-offs in collecting/releasing data) to help participants gain a correct mental model of collected data. It is important to deal with the trade-offs in terms of soundness and completeness in illustrating data collection practices as stated in a prior mental model study [48].

5.2.2 Dynamic Consent. Providing flexible and fine-grained control will play a more active role in shaping participant involvement in data collection and release. From our interview analysis, we found that simple informed consent based on a yes/no item does not live up to complex privacy implications, as participants' perceived data sensitivity differed based on their contexts. Efforts toward designing a "*just-in-time*" information related to informed consent should be considered, by designing a system that makes inquiries on participants' available contexts. The basic concept is very similar to context-aware privacy notices [27, 40], but we can extend this by adopting "dynamic consent," which refers to a personalized, digital platform that allows participants to tailor and manage their own consent preferences [43]. Dynamic consent is a promising design approach for

flexible control of data management. Our results showed that participants' privacy concerns varied according to their context. Likewise, the life cycle of consents can change over time, dynamic consent offers context-aware data management that enables *withhold-grant-revoke-amend* consent in everyday life contexts[51]. Introducing automated tools may help improve adoption of dynamic consent techniques in open dataset collection settings; for example, context-aware rules in the form of trigger action programming [6] can be considered to enable rule-based automated privacy decision making.

5.3 Limitation

One caveat of our results is that the current dataset was largely collected from students in a large research-oriented university as in prior studies [29, 97, 98], which may have caused self-selection bias. Although participants generally showed positive responses toward two key motives (i.e., financial and altruistic motives), such attitudes may not be generalizable to other participants from an external institution or participants who are not a member of a scientific community, or are with different socio-economic status. To mitigate such potential bias, further studies on different target groups are required to generalize our findings and prevent potential self-selection bias [85]. One possible consideration is recruiting a wide range of participants who engage in the different nature of the contexts compared to other participants. Collecting sensor data from a broader range of people (e.g., the Tesserae project [60]) would likely provide a more diverse dataset that reflects multifaceted aspects of in-the-wild contexts (e.g., identifying new themes of privacy concerns, privacy-sensitive contexts), thus contributing to the diversity of datasets. It is also worth considering exploring cross-cultural differences (e.g., collectivist vs. individualistic cultures [35]) in open dataset projects. We posit that our results on motives and concerns will be applicable to different cultural contexts because similar results have been verified in studies performed in western countries (e.g., personal data sharing for bio research) [14, 82].

6 CONCLUSION

We have taken a mixed-method approach to studying participants' attitudes and privacy concerns in an open dataset collection project for affective computing research. From our large-scale exploratory study in the wild (N = 100, 4 weeks), we found that participant motives (i.e. financial and altruistic) and diverse types of privacy concerns played a pivotal role in shaping participants' attitudes toward open dataset collection. Our qualitative analysis of in-depth interview data from participants revealed participants' sensor-specific "intuitive concerns" due to potential revelation of personal traits and social behaviors (e.g., calls, texts, app usage, and GPS). Participants' privacy attitudes were largely dependent upon their perception on judgment/categorization and surveillance. However, the participants were largely unconcerned with privacy risks, owing to misconceptions about data control and a lack of proper mental models in sensor data collection. We discussed data contributors' behaviors in open dataset collection and suggested several approaches to promote data contributors' motivations. We argued the need of "context-aware privacy support" for open dataset collection with mobile and wearable devices. Put together, we hope that our findings bring novel insights into promoting active and privacy-aware open dataset collection practices within the HCI research communities.

ACKNOWLEDGMENTS

This research was supported by the Bio & Medical Technology Development Program of the National Research Foundation (NRF) funded by the Korean government (MSIT) (No. 2021M3A9E4080780) and by the Basic Science Research Program through NRF funded by MSIT (No. 2020R1A4A1018774, 2022R1A2C2011536).

REFERENCES

[1] Mojtaba Khomami Abadi, Ramanathan Subramanian, Seyed Mostafa Kia, Paolo Avesani, Ioannis Patras, and Nicu Sebe. 2015. DECAF: MEG-based multimodal database for decoding affective physiological responses. *IEEE Transactions on Affective Computing* 6, 3 (2015),

209–222.
[2] Gregory D Abowd, Anind K Dey, Peter J Brown, Nigel Davies, Mark Smith, and Pete Steggles. 1999. Towards a better understanding of context and context-awareness. In *International symposium on handheld and ubiquitous computing*. Springer, New York, NY, USA, 304–307.
[3] Mark S Ackerman, Lorrie Faith Cranor, and Joseph Reagle. 1999. Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM Conference on Electronic Commerce*. ACM, New York, NY, USA, 1–8.
[4] Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE security & privacy* 3, 1 (2005), 26–33.
[5] Alessandro Acquisti, Leslie K John, and George Loewenstein. 2013. What is privacy worth? *The Journal of Legal Studies* 42, 2 (2013), 249–274.
[6] Unai Alegre, Juan Carlos Augusto, and Tony Clark. 2016. Engineering context-aware systems and applications: A survey. *Journal of Systems and Software* 117 (2016), 55–83.
[7] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your location has been shared 5,398 times! A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. ACM, New York, NY, USA, 787–796.
[8] Andy Alorwu, Saba Kheirinejad, Niels van Berkel, Marianne Kinnula, Denzil Ferreira, Aku Visuri, and Simo Hosio. 2021. Assessing MyData Scenarios: Ethics, Concerns, and the Promise. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–11.
[9] Abdulmajeed Alqhatani and Heather Richter Lipford. 2019. "There is nothing that I need to keep secret": Sharing Practices and Concerns of Wearable Fitness Data. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*. 421–434.
[10] appleheart. 2021. *appleheart*. https://med.stanford.edu/appleheartstudy.html
[11] Mehrdad Bahrini, Nina Wenig, Marcel Meissner, Karsten Sohr, and Rainer Malaka. 2019. HappyPerMi: Presenting critical data flows in mobile application to raise user security awareness. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–6.
[12] Oresti Baños, Miguel Damas, Héctor Pomares, Ignacio Rojas, Máté Attila Tóth, and Oliver Amft. 2012. A benchmark dataset to evaluate sensor displacement in activity recognition. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. 1026–1035.
[13] C Daniel Batson, Nadia Ahmad, and Jo-Ann Tsang. 2002. Four motives for community involvement. *Journal of social issues* 58, 3 (2002), 429–445.
[14] Elizabeth A Bell, Lucila Ohno-Machado, and M Adela Grando. 2014. Sharing my health data: a survey of data sharing preferences of healthy individuals. In *AMIA annual symposium proceedings*, Vol. 2014. American Medical Informatics Association, 1699.
[15] Dror Ben-Zeev, Emily A Scherer, Rui Wang, Haiyi Xie, and Andrew T Campbell. 2015. Next-generation psychiatric assessment: Using smartphone sensors to monitor behavior and mental health. *Psychiatric rehabilitation journal* 38, 3 (2015), 218.
[16] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced confidences: Privacy and the control paradox. *Social psychological and personality science* 4, 3 (2013), 340–347.
[17] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.
[18] Luca Canzian and Mirco Musolesi. 2015. Trajectories of depression: unobtrusive monitoring of depressive states by means of smartphone mobility traces analysis. In *Proceedings of the 2015 ACM international joint conference on pervasive and ubiquitous computing*. 1293–1304.
[19] Delphine Christin. 2016. Privacy in mobile participatory sensing: Current trends and future challenges. *Journal of Systems and Software* 116 (2016), 57–68.
[20] Sheldon Cohen, Tom Kamarck, and Robin Mermelstein. 1983. A global measure of perceived stress. *Journal of health and social behavior* (1983), 385–396.
[21] Sunny Consolvo, David W McDonald, Tammy Toscos, Mike Y Chen, Jon Froehlich, Beverly Harrison, Predrag Klasnja, Anthony LaMarca, Louis LeGrand, Ryan Libby, et al. 2008. Activity sensing in the wild: a field trial of ubifit garden. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 1797–1806.
[22] Martin Cooney, Sepideh Pashami, Anita Sant'Anna, Yuantao Fan, and Slawomir Nowaczyk. 2018. Pitfalls of Affective Computing: How can the automatic visual communication of emotions lead to harm, and what can be done to mitigate such risks. In *Companion Proceedings of the The Web Conference 2018*. 1563–1566.
[23] Yves-Alexandre de Montjoye, Jordi Quoidbach, Florent Robic, and Alex Sandy Pentland. 2013. Predicting personality using novel mobile phone-based metrics. In *International conference on social computing, behavioral-cultural modeling, and prediction*. Springer, New York, NY, USA, 48–55.
[24] Mohammad Omar Derawi, Claudia Nickel, Patrick Bours, and Christoph Busch. 2010. Unobtrusive user-authentication on mobile phones using biometric gait recognition. In *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 306–311.
[25] Anind K Dey. 2001. Understanding and using context. *Personal and ubiquitous computing* 5, 1 (2001), 4–7.

[26] Nathan Eagle and Alex Sandy Pentland. 2006. Reality mining: sensing complex social systems. *Personal and ubiquitous computing* 10, 4 (2006), 255–268.
[27] Nico Ebert, Kurt Alexander Ackermann, and Björn Scheppler. 2021. Bolder is Better: Raising User Awareness through Salient and Concise Privacy Notices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–12.
[28] Anja Exler, Andrea Schankin, Christoph Klebsattel, and Michael Beigl. 2016. A wearable system for mood assessment considering smartphone features and data from mobile ECGs. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*. ACM, New York, NY, USA, 1153–1161.
[29] Asma Ahmad Farhan, Chaoqun Yue, Reynaldo Morillo, Shweta Ware, Jin Lu, Jinbo Bi, Jayesh Kamath, Alexander Russell, Athanasios Bamis, and Bing Wang. 2016. Behavior vs. introspection: refining prediction of clinical depression via smartphone sensing data. In *2016 IEEE Wireless Health (WH)*. IEEE, 1–8.
[30] Jon Froehlich, Mike Y Chen, Sunny Consolvo, Beverly Harrison, and James A Landay. 2007. MyExperience: a system for in situ tracing and capturing of user feedback on mobile phones. In *Proceedings of the 5th international conference on Mobile systems, applications and services*. 57–70.
[31] Sandra Gabriele and Sonia Chiasson. 2020. Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–12.
[32] Nanna Gorm and Irina Shklovski. 2016. Sharing steps in the workplace: Changing privacy concerns over time. In *proceedings of the 2016 CHI conference on human factors in computing systems*. 4315–4319.
[33] Agnes Grünerbl, Amir Muaremi, Venet Osmani, Gernot Bahle, Stefan Oehler, Gerhard Tröster, Oscar Mayora, Christian Haring, and Paul Lukowicz. 2014. Smartphone-based recognition of states and state changes in bipolar disorder patients. *IEEE Journal of Biomedical and Health Informatics* 19, 1 (2014), 140–148.
[34] Gabriella M Harari, Samuel D Gosling, RUI Wang, and Andrew T Campbell. 2015. Capturing situational information with smartphones and mobile sensing methods. *European Journal of Personality* 29, 5 (2015), 509–511.
[35] Geert Hofstede, Gert Jan Hofstede, and Michael Minkov. 2005. *Cultures and organizations: Software of the mind*. Vol. 2. Mcgraw-hill New York.
[36] Karen Hovsepian, Mustafa al'Absi, Emre Ertin, Thomas Kamarck, Motohiro Nakajima, and Santosh Kumar. 2015. cStress: towards a gold standard for continuous stress assessment in the mobile environment. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, New York, NY, USA, 493–504.
[37] Bernardo A Huberman, Eytan Adar, and Leslie R Fine. 2005. Valuating privacy. *IEEE security & privacy* 3, 5 (2005), 22–25.
[38] Princely Ifinedo. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* 31, 1 (2012), 83–95.
[39] Thomas R Insel. 2017. Digital phenotyping: technology for a new science of behavior. *Jama* 318, 13 (2017), 1215–1216.
[40] Corey Brian Jackson and Yang Wang. 2018. Addressing the privacy paradox through personalized privacy notifications. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies* 2, 2 (2018), 1–25.
[41] Luis G Jaimes, Idalides J Vergara-Laurens, and Andrew Raij. 2015. A survey of incentive techniques for mobile crowd sensing. *IEEE Internet of Things Journal* 2, 5 (2015), 370–380.
[42] Matthew Kay, Eun Kyoung Choe, Jesse Shepherd, Benjamin Greenstein, Nathaniel Watson, Sunny Consolvo, and Julie A Kientz. 2012. Lullaby: a capture & access system for understanding the sleep environment. In *Proceedings of the 2012 ACM conference on ubiquitous computing*. 226–234.
[43] Jane Kaye, Edgar A Whitley, David Lund, Michael Morrison, Harriet Teare, and Karen Melham. 2015. Dynamic consent: a patient interface for twenty-first century research networks. *European journal of human genetics* 23, 2 (2015), 141–146.
[44] Ji-Hyeon Kim, Bok-Hwan Kim, and Moon-Sun Ha. 2011. Validation of a Korean version of the Big Five Inventory. *Journal of Human Understanding and Counseling* 32, 1 (2011), 47–65.
[45] Seoyoung Kim, Arti Thakur, and Juho Kim. 2020. Understanding Users' Perception Towards Automated Personality Detection with Group-specific Behavioral Data. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–12.
[46] David M Kreps. 1997. Intrinsic motivation and extrinsic incentives. *The American economic review* 87, 2 (1997), 359–364.
[47] Kurt Kroenke, Robert L Spitzer, and Janet BW Williams. 2001. The PHQ-9: validity of a brief depression severity measure. *Journal of general internal medicine* 16, 9 (2001), 606–613.
[48] Todd Kulesza, Simone Stumpf, Margaret Burnett, Sherry Yang, Irwin Kwan, and Weng-Keen Wong. 2013. Too much, too little, or just right? Ways explanations impact end users' mental models. In *2013 IEEE Symposium on visual languages and human centric computing*. IEEE, 3–10.
[49] Jennifer R Kwapisz, Gary M Weiss, and Samuel A Moore. 2011. Activity recognition using cell phone accelerometers. *ACM SigKDD Explorations Newsletter* 12, 2 (2011), 74–82.
[50] Reed Larson and Mihaly Csikszentmihalyi. 1983. The Experience Sampling Method. *New Directions for Methodology of Social & Behavioral Science* (1983).

[51] Hyunsoo Lee and Uichin Lee. 2021. Dynamic Consent for Sensor-Driven Research. In *2021 Thirteenth International Conference on Mobile Computing and Ubiquitous Network (ICMU)*. IEEE, 1–6.

[52] Ja-Young Lee, Suk-Kyung Nam, Mi-Kyoung Lee, Ji-Hee Lee, and SM Lee. 2009. Rosenberg'self-esteem scale: analysis of item-level validity. *Korean J Couns Psychother* 21, 1 (2009), 173–189.

[53] Uichin Lee, Jihyoung Kim, Eunhee Yi, Juyup Sung, and Mario Gerla. 2013. Analyzing crowd workers in mobile pay-for-answer q&a. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 533–542.

[54] Robert LiKamWa, Yunxin Liu, Nicholas D Lane, and Lin Zhong. 2013. Moodscope: Building a mood sensor from smartphone usage patterns. In *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*. ACM, New York, NY, USA, 389–402.

[55] TH Lim. 2014. Validation of the korean version of positive psychological capital (K-PPC). *Journal of coaching development* 16, 3 (2014), 157–166.

[56] Young Jin Lim. 2012. Psychometric properties of the satisfaction with life scale among Korean police officers, university students, and adolescents. *Korean Journal of Psychology: General* 31, 3 (2012), 877–896.

[57] Chang Liu, Jack T Marchewka, June Lu, and Chun-Sheng Yu. 2005. Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management* 42, 2 (2005), 289–304.

[58] Byron Lowens, Vivian Genaro Motti, and Kelly Caine. 2017. Wearable privacy: Skeletons in the data closet. In *2017 IEEE international conference on healthcare informatics (ICHI)*. IEEE, 295–304.

[59] A Lundin, M Hallgren, H Theobald, C Hellgren, and Margareta Torgén. 2016. Validity of the 12-item version of the General Health Questionnaire in detecting depression in the general population. *Public health* 136 (2016), 66–74.

[60] Stephen M Mattingly, Julie M Gregg, Pino Audia, Ayse Elvan Bayraktaroglu, Andrew T Campbell, Nitesh V Chawla, Vedant Das Swain, Munmun De Choudhury, Sidney K D'Mello, Anind K Dey, et al. 2019. The Tesserae project: Large-scale, longitudinal, in situ, multimodal sensing of information workers. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–8.

[61] Abhinav Mehrotra, Fani Tsapeli, Robert Hendley, and Mirco Musolesi. 2017. MyTraces: Investigating Correlation and Causation between Users' Emotional States and Mobile Phone Interaction. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 3 (2017), 83.

[62] David L Mothersbaugh, William K Foxx, Sharon E Beatty, and Sijun Wang. 2012. Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of service research* 15, 1 (2012), 76–98.

[63] Vivian Genaro Motti and Kelly Caine. 2015. Users' privacy concerns about wearables. In *International Conference on Financial Cryptography and Data Security*. Springer, New York, NY, USA, 231–244.

[64] Mohamed Musthag, Andrew Raij, Deepak Ganesan, Santosh Kumar, and Saul Shiffman. 2011. Exploring micro-incentive strategies for participant compensation in high-burden studies. In *Proceedings of the 13th international conference on Ubiquitous computing*. 435–444.

[65] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an IoT world. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 399–412.

[66] Jennifer Nicholas, Katie Shilton, Stephen M Schueller, Elizabeth L Gray, Mary J Kwasny, and David C Mohr. 2019. The role of data type and recipient in individuals' perspectives on sharing passively collected smartphone data for mental health: Cross-sectional questionnaire study. *JMIR mHealth and uHealth* 7, 4 (2019), e12578.

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

[68] Jill M Oliver, MJ Slashinski, T Wang, PA Kelly, SG Hilsenbeck, and AL McGuire. 2012. Balancing the risks and benefits of genomic data sharing: genome research participants' perspectives. *Public health genomics* 15, 2 (2012), 106–114.

[69] Jukka-Pekka Onnela and Scott L Rauch. 2016. Harnessing smartphone-based digital phenotyping to enhance behavioral and mental health. *Neuropsychopharmacology* 41, 7 (2016), 1691–1696.

[70] Cheul Young Park, Narae Cha, Soowon Kang, Auk Kim, Ahsan Habib Khandoker, Leontios Hadjileontiadis, Alice Oh, Yong Jeong, and Uichin Lee. 2020. K-EmoCon, a multimodal sensor dataset for continuous emotion recognition in naturalistic conversations. *Scientific Data* 7, 1 (2020), 1–16.

[71] Sangkeun Park, Joohyun Kim, Rabeb Mizouni, and Uichin Lee. 2016. Motives and concerns of dashcam video sharing. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 4758–4769.

[72] Eyal Peer, Serge Egelman, Marian Harbach, Nathan Malkin, Arunesh Mathur, and Alisa Frik. 2020. Nudge me right: Personalizing online security nudges to people's decision-making styles. *Computers in Human Behavior* 109 (2020), 106347.

[73] Chanda Phelan, Cliff Lampe, and Paul Resnick. 2016. It's creepy, but it doesn't bother me. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 5240–5251.

[74] Svenja Pieritz, Mohammed Khwaja, A Aldo Faisal, and Aleksandar Matic. 2021. Personalised Recommendations in Mental Health Apps: The Impact of Autonomy and Data Sharing. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–12.

[75] Aarathi Prasad, Jacob Sorber, Timothy Stablein, Denise Anthony, and David Kotz. 2012. Understanding sharing preferences and behavior for mHealth devices. In *Proceedings of the 2012 ACM workshop on Privacy in the electronic society*. 117–128.

[76] Sasank Reddy, Deborah Estrin, Mark Hansen, and Mani Srivastava. 2010. Examining micro-payments for participatory sensing data collections. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*. 33–36.
[77] Ronald W Rogers. 1975. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology* 91, 1 (1975), 93–114.
[78] John Rooksby, Alistair Morrison, and Dave Murray-Rust. 2019. Student perspectives on digital phenotyping: The acceptability of using smartphone data to assess mental health. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–14.
[79] Dominik Rüegger, Mirjam Stieger, Marcia Nißen, Mathias Allemand, Elgar Fleisch, and Tobias Kowatsch. 2020. How are personality states associated with smartphone data? *European Journal of Personality* 34, 5 (2020), 687–713.
[80] Sohrab Saeb, Mi Zhang, Christopher J Karr, Stephen M Schueller, Marya E Corden, Konrad P Kording, and David C Mohr. 2015. Mobile phone sensor correlates of depressive symptom severity in daily-life behavior: an exploratory study. *Journal of medical Internet research* 17, 7 (2015), e175.
[81] Maude Schneider, Thomas Vaessen, Esther DA van Duin, Zuzana Kasanova, Wolfgang Viechtbauer, Ulrich Reininghaus, Claudia Vingerhoets, Jan Booij, Ann Swillen, Jacob AS Vorstman, et al. 2020. Affective and psychotic reactivity to daily-life stress in adults with 22q11DS: a study using the experience sampling method. *Journal of Neurodevelopmental Disorders* 12, 1 (2020), 1–11.
[82] Nisha Shah, Victoria Coathup, Harriet Teare, Ian Forgie, Giuseppe Nicola Giordano, Tue Haldor Hansen, Lenka Groeneveld, Michelle Hudson, Ewan Pearson, Hartmut Ruetten, et al. 2019. Motivations for data sharing—views of research participants from four European countries: a DIRECT study. *European Journal of Human Genetics* 27, 5 (2019), 721–729.
[83] Ruth Shillair, Shelia R Cotten, Hsin-Yi Sandy Tsai, Saleem Alhabash, Robert LaRose, and Nora J Rifon. 2015. Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior* 48 (2015), 199–207.
[84] Sarah Spiekermann, Jens Grossklags, and Bettina Berendt. 2001. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce*. 38–47.
[85] Peter M Steiner, Thomas D Cook, William R Shadish, and Margaret H Clark. 2010. The importance of covariate selection in controlling for selection bias in observational studies. *Psychological methods* 15, 3 (2010), 250.
[86] Artem Timoshenko and John R Hauser. 2019. Identifying customer needs from user-generated content. *Marketing Science* 38, 1 (2019), 1–20.
[87] John Torous, Hannah Wisniewski, Bruce Bird, Elizabeth Carpenter, Gary David, Eduardo Elejalde, Dan Fulford, Synthia Guimond, Ryan Hays, Philip Henson, et al. 2019. Creating a digital health smartphone app and digital phenotyping platform for mental health and diverse healthcare needs: an interdisciplinary and collaborative approach. *Journal of Technology in Behavioral Science* 4, 2 (2019), 73–85.
[88] Tammy Toscos, Anne Faber, Shunying An, and Mona Praful Gandhi. 2006. Chick clique: persuasive technology to motivate teenage girls to exercise. In *Extended Abstracts of the 2006 CHI Conference on Human Factors in Computing Systems*. 1873–1878.
[89] Yonatan Vaizman, Katherine Ellis, and Gert Lanckriet. 2017. Recognizing detailed human context in the wild from smartphones and smartwatches. *IEEE pervasive computing* 16, 4 (2017), 62–74.
[90] Yonatan Vaizman, Katherine Ellis, Gert Lanckriet, and Nadir Weibel. 2018. Extrasensory app: Data collection in-the-wild with rich user interface to self-report behavior. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.
[91] René van Bavel, Nuria Rodríguez-Priego, José Vila, and Pam Briggs. 2019. Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies* 123 (2019), 29–39.
[92] Paul Voigt and Axel Von dem Bussche. 2017. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing* 10 (2017), 3152676.
[93] Daniel T Wagner, Andrew Rice, and Alastair R Beresford. 2014. Device Analyzer: Large-scale mobile data collection. *ACM SIGMETRICS Performance Evaluation Review* 41, 4 (2014), 53–56.
[94] Fabian Wahle, Lea Bollhalder, Tobias Kowatsch, and Elgar Fleisch. 2017. Toward the design of evidence-based mental health information systems for people with depression: a systematic literature review and meta-analysis. *Journal of medical internet research* 19, 5 (2017), e191.
[95] Fabian Wahle, Tobias Kowatsch, Elgar Fleisch, Michael Rufer, and Steffi Weidt. 2016. Mobile sensing and support for people with depression: a pilot trial in the wild. *JMIR mHealth and uHealth* 4, 3 (2016), e5960.
[96] Julie B Wang, Jeffrey E Olgin, Gregory Nah, Eric Vittinghoff, Janine K Cataldo, Mark J Pletcher, and Gregory M Marcus. 2018. Cigarette and e-cigarette dual use and risk of cardiopulmonary symptoms in the Health eHeart Study. *PloS one* 13, 7 (2018), e0198681.
[97] Rui Wang, Fanglin Chen, Zhenyu Chen, Tianxing Li, Gabriella Harari, Stefanie Tignor, Xia Zhou, Dror Ben-Zeev, and Andrew T Campbell. 2014. StudentLife: assessing mental health, academic performance and behavioral trends of college students using smartphones. In *Proceedings of the 2014 ACM international joint conference on pervasive and ubiquitous computing*. 3–14.
[98] Rui Wang, Gabriella Harari, Peilin Hao, Xia Zhou, and Andrew T Campbell. 2015. SmartGPA: how smartphones can assess and predict academic performance of college students. In *Proceedings of the 2015 ACM international joint conference on pervasive and ubiquitous computing*. 295–306.

[99] Rui Wang, Weichen Wang, Alex DaSilva, Jeremy F Huckins, William M Kelley, Todd F Heatherton, and Andrew T Campbell. 2018. Tracking depression dynamics in college students using mobile phone and wearable sensing. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 1 (2018), 1–26.

[100] Raf Widdershoven, Marieke Wichers, Peter Kuppens, Jessica Hartmann, Claudia Menne-Lothmann, Claudia Simons, and Jojanneke Bastiaansen. 2019. Effect of self-monitoring through experience sampling on emotion differentiation in depression. *Journal of Affective Disorders* (2019), 71–77.

[101] Michael Workman, William H Bommer, and Detmar Straub. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior* 24, 6 (2008), 2799–2816.

[102] Heng Xu, Tamara Dinev, H Jeff Smith, and Paul Hart. 2008. Examining the formation of individual's privacy concerns: Toward an integrative view. (2008).

[103] Heng Xu, Sumeet Gupta, Mary Beth Rosson, and John M Carroll. 2012. Measuring mobile users' concerns for information privacy. (2012).

[104] Xuhai Xu, Prerna Chikersal, Afsaneh Doryab, Daniella K Villalba, Janine M Dutcher, Michael J Tumminia, Tim Althoff, Sheldon Cohen, Kasey G Creswell, J David Creswell, et al. 2019. Leveraging routine behavior and contextually-filtered features for depression detection among college students. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 3 (2019), 1–33.

[105] Seounmi Youn. 2005. Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media* 49, 1 (2005), 86–110.

[106] Xinglin Zhang, Zheng Yang, Wei Sun, Yunhao Liu, Shaohua Tang, Kai Xing, and Xufei Mao. 2015. Incentives for mobile crowd sensing: A survey. *IEEE Communications Surveys & Tutorials* 18, 1 (2015), 54–67.

[107] Mingmin Zhao, Fadel Adib, and Dina Katabi. 2016. Emotion recognition using wireless signals. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*. 95–108.

[108] Yixin Zou and Florian Schaub. 2018. Concern But No Action: Consumers' Reactions to the Equifax Data Breach. In *Extended abstracts of the 2018 CHI conference on human factors in computing systems*. 1–6.