PriviAware: Exploring Data Visualization and Dynamic Privacy Control Support for Data Collection in Mobile Sensing Research

Hyunsoo Lee
KAIST
Daejeon, Republic of Korea
hslee90@kaist.ac.kr

Yugyeong Jung
KAIST
Daejeon, Republic of Korea
yugyeong.jung@kaist.ac.kr

Hei Yiu Law
KAIST
Daejeon, Republic of Korea
emilyelhy@yahoo.com

Seolyeong Bae
GIST
Gwangju, Republic of Korea
seolyeongbae@gm.gist.ac.kr

Uichin Lee*
KAIST
Daejeon, Republic of Korea
uclee@kaist.ac.kr

ABSTRACT

With increased interest in leveraging personal data collected from 24/7 mobile sensing for digital healthcare research, supporting user-friendly consent to data collection for user privacy has also become important. This work proposes *PriviAware*, a mobile app that promotes flexible user consent to data collection with data exploration and contextual filters that enable users to turn off data collection based on time and places that are considered privacy-sensitive. We conducted a user study (N = 58) to explore how users leverage data exploration and contextual filter functions to explore and manage their data and whether our system design helped users mitigate their privacy concerns. Our findings indicate that offering fine-grained control is a promising approach to raising users' privacy awareness under the dynamic nature of the pervasive sensing context. We provide practical privacy-by-design guidelines for mobile sensing research.

CCS CONCEPTS

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

KEYWORDS

Mobile Sensing Research, Sensor Data Collection, Usable Privacy

ACM Reference Format:
Hyunsoo Lee, Yugyeong Jung, Hei Yiu Law, Seolyeong Bae, and Uichin Lee. 2024. PriviAware: Exploring Data Visualization and Dynamic Privacy Control Support for Data Collection in Mobile Sensing Research. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3613904.3642815

*Corresponding author

CHI '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642815

1 INTRODUCTION

Mobile sensing has been an intrinsic part of ubiquitous computing, which has weaved itself into the fabric of our everyday life [83]. Recently, there has been a growing realization in academia that everyday mobile phones, which passively collect and analyze behavioral sensor data 24/7, can contribute to understanding relationships between people's daily behaviors and debilitating health challenges (e.g., depression [57, 76]). Studies have shown that this promising approach, also known as *digital phenotyping*, provides a continuous and passive assessment of one's behavior, mood, and cognition by applying machine learning to physiological and biometric data collected from smartphones and other personal digital devices [30]. Thus far, most published studies that leverage mobile sensing have focused on many behavioral issues and mental health, such as schizophrenia [8], mood disorder [76], sleep disorder [73], depression [68] and suicide prevention [37].

To assess one's mental health status or identify the predictors of mental health risks, acquiring data is the first part of mobile sensing research. Generally, the study involves massive amounts of personal data collection from smartphones and other digital wearables. For example, various digital biomarkers that are being utilized in mobile sensing research for mental health are geolocation, calls (outgoing/incoming duration/timing), messages (length/timing), finger taps (speed, number), phone status (WiFi, Bluetooth, battery charging, power on/off state), accelerometer, sleep, heart rate/variability, app usage and so on [77, 82].

Due to such a passive and massive collection of user data and the process of transforming one's daily footage into health information using artificial intelligence, data collection in mobile sensing is riddled with ethical privacy and transparency issues. One novel challenge posed by such mobile sensing research arises from its passive sensing that collects and generates health-related information outside the clinical setting. For example, while seemingly mundane data generated within daily contexts can turn into powerful indicators of mental functions (e.g., keystroke patterns [52]), people do not ordinarily associate these data with healthcare and thus are not necessarily protected by existing standards [22, 52]. Furthermore, data sources that are highly granular and indicative of one's social interactions (e.g., GPS, call/text logs) can increase the likelihood of identifiability when combined with other personal sensor readings (e.g., heart rate, accelerometer, WiFi data) [22, 40]. Protecting user data and ensuring privacy is especially critical in

mobile sensing research because the sensitivity of behavioral and mental health diagnoses and predictions may impact employment, insurance, litigation, or other occasions [52]. Furthermore, collecting every data trace generated by an individual leads to detailed inferences about one's private life (e.g., accelerometer data revealing current activities [38], as well as surveillance of individuals).

Despite such concerns, recent studies have demonstrated that a large number of participants involved in mobile sensing research would often underestimate the severity of potential privacy threats due to limited knowledge of sensor data and showed difficulty recalling diverse types of sensor data and associating them with potential privacy risks that can occur to them [40, 41, 64]. Studies have pointed out that such lack of privacy awareness occurs due to a lack of transparency in mobile sensing research [52, 61], as sensor data collection and its processing are often not articulated or easily examined by outsiders [52]. Since sensor data collection for mental health research and its consequences are new and largely unknown to participants, researchers should describe precisely to research subjects what data is collected, how it is collected, and when it is collected in the informed consent process. Researchers of relevant studies have pointed out that future studies should actively explore consent mechanisms that increase users' privacy awareness and support user-friendly consent to data collection in mobile sensing contexts [40–42].

While such mobile sensing studies have called for further research and discourse on how supporting technologies should be designed and implemented to minimize the potential privacy risks in mobile sensing, existing HCI studies have centered around personal data privacy in terms of mobile application usage and its permission [46, 47, 84]. For example, prior studies have focused on limited types of data privacy (e.g., social interaction and GPS) for mobile application services rather than comprehensive mobile sensor data collection for research purposes. Under this context, simple notice (e.g., privacy policy visualization [24] or diversified privacy notices [18, 31, 34, 35]), and partial user control in terms of data sharing (usually per-app basis) have been suggested as a design mechanism to increase user awareness to privacy threats and support users' privacy decision making. Considering that individuals' everyday footprints are being collected through mobile sensing for mental health analysis regardless of their intentions, we find that existing design approaches are relatively static and less engaging to compensate for novel privacy threats due to continuous sensing.

To cope with such limitations, recent pervasive sensing studies have suggested designing user-friendly consent mechanisms that can support more fine-grained and flexible data collection options so that they could selectively disable data collection in privacy-sensitive contexts (e.g., visiting a hospital) [41]. Given that users are generally inattentive to potential privacy threats due to a lack of knowledge and transparency in mobile sensor data collection, it also suggests a need for an explanatory feature that can inform users of the diverse sensor data types [40]. This echoes arguments from previous works on mobile sensing for mental health, which claim that comprehension and voluntariness are challenges that must not be overlooked across mental health applications for mobile sensing research [52].

Considering this, we take a step forward and envision a system design that supports flexible consent to sensor data collection for mobile sensing research. In this study, we design and evaluate *PriviAware* to explore the design space of the feasibility of privacy-by-design for mobile dataset collection with context-aware privacy support. A combination of data exploration and contextual filtering informs participants of the overview of their personal data collection and its usage (i.e., data exploration) and supports participants in proactively configuring their data collection consent based on their contextual preferences (i.e., contextual filtering). We iteratively prototyped *PriviAware* and conducted an exploratory field study with two different intervention groups (Group A: Data exploration, Group B: Data exploration + Contextual filtering, N = 58) for three weeks. After three weeks of the experiment, we investigated user experiences of PriviAware with two different intervention conditions.

Our in-depth investigation shows that participants from both groups would report increased perceived privacy concerns and awareness due to the data exploration feature. Furthermore, we find that participants from group B, who were also provided with contextual filtering, reported a sense of empowerment regarding their privacy rights and actively leveraged the feature to manage and protect their data in their daily lives. Our findings helped us to explore several practical design directions, such as considering automated context-awareness support to reduce decision fatigue and exploring and enabling data-driven actionable insights for personal data management. Overall, our preliminary study explores a novel design approach that supports participants' consent to sensitive data collection and responsible personal data management. To the best of our knowledge, PriviAware is the first to explicitly visualize and allow for contextual controls on what mobile sensing data is being continuously shared with researchers and app developers.

The key contributions of our study are as follows:

- We present *PriviAware*, a mobile intervention app for promoting participants' proactive data collection consent and privacy management within the mobile sensing context for digital healthcare research. We aimed to create a more inclusive and engaging user experience by designing the system with transparent and detailed information on data collection along with greater privacy empowerment. The system is available at Github[1]
- We conducted the three-week deployment study in the wild, which we consider a preliminary study that empirically demonstrated that the visualization of sensor data improved users' privacy awareness, and contextual filtering improved users' perceived empowerment in mobile sensing contexts.
- We discussed design implications on how current consent mechanisms can be improved and facilitated to increase transparency and user empowerment in making privacy-informed decisions.

2 BACKGROUND AND RELATED WORK

2.1 Mobile Sensing Research and Privacy Concerns

2.1.1 Personal data collection for mobile sensing research. Harnessing large-scale mobile data collected via 24/7 sensing for health-related

[1] https://github.com/Kaist-ICLab/PriviAware-App.git

research has been one of the popular research topics in HCI and ubiquitous computing. Collected sensor readings of the data can be leveraged as behavioral biomarkers (e.g., sleep, physical activities) that support the inference of an individual's behavioral patterns for diagnosis, treatment, and clinical support [71, 76]. This data-driven approach, also known as *digital phenotyping*, has been actively pursued to facilitate digital healthcare research. Notably, extensive research has been done to explore the relationship between mobile sensor data and one's mental health, such as mood disorder [76], depression [75, 76, 89], or stress [67, 79]. One representative example of digital phenotyping studies is the StudentLife project, which has demonstrated that smartphone sensor data, such as Bluetooth and GPS logs, are associated with the stress level of college students [81]. Saeb et al. discovered that mobile sensor data like GPS or smartphone usage history could serve as behavioral markers for depressive symptoms [66]. Another study found that accelerometer sensor data collected from a smartphone keyboard is related to the variation of mood and cognition [55]. Regarding physical health, eHeart Study leverages smartphone heart rate, weight, sleep patterns, and physical activity to analyze and predict heart-related diseases [60, 80].

2.1.2 Privacy concerns in mobile sensor data collection. Despite the novel opportunities that mobile sensing can offer, passive sensor data collection often puts the participants' privacy at stake. This is because collecting such naturalistic data from one's daily life becomes sensitive due to the diversity of personal data; e.g., biometric data (e.g., heart rate), behavioral data (e.g., mobility), contexts (e.g., GPS location and timestamps), and extra user data (e.g., self-reports about mood and stress). The ubiquitous nature of pervasive sensing makes it challenging to protect user privacy because data can be constantly collected.

Recent studies have explored privacy concerns in sensor data collection from participants' perspectives. For example, Rooksby et al.'s study explored college students' acceptability and privacy concerns in digital phenotyping's passive sensing for mental health and well-being [64]. Similarly, Lee et al.'s study on university students' perceived risks toward mobile and wearable sensor data collection for research purposes has revealed that participants' privacy concerns center around personal profiling (e.g., routine identification), judgment on one's traits, fear of surveillance, and potential data abuse [40]. Such concerns on mobile sensing tend to grow over time as combining multiple sensor streams enables the inference of detailed behavioral patterns and even re-identification of anonymous data providers [53, 62]. For example, previous research has indicated innocuous information (e.g., step counts) can also cause privacy concerns when interconnected with different social contexts [22].

While such privacy concerns exist, much of the prior work has demonstrated that participants would compensate for their privacy for several reasons. One primary reason is participants' limited understanding and incomplete mental models in sensor data collection practices (e.g., data collection types, purposes, etc.) [40, 41]. For example, participants from mobile sensing research reported difficulty understanding each sensor data and its association with one's mental health, rendering them to sacrifice their data [40] easily. Participants would also outweigh financial compensation than the value of their data, which is known as privacy-utility trade-off [29, 40].

With such concerns and participant observations on their privacy-decision-making call for more user-friendly privacy support, a large body of existing sensing platforms and applications have primarily focused on data encryption, a security method that allows data encoding that can only be decoded with the correct encryption key [7, 20, 27, 45, 74], while only a few offer user-friendly consent [4] or provide users with an option to suspend privacy-sensitive data collection [28] (see Table 1). Given such limitations, we aimed to design a system that allows for more user-centered control and user-friendly and easy-to-understand guidance.

2.2 Usable privacy support for mobile sensing research

2.2.1 HCI studies for usable privacy. While it has been observed that people compromise their personal data protection due to the knowledge disparity between researchers and participants, several streams of HCI research have explored system design approaches that inform users of potential privacy concerns and raise users' privacy awareness. However, existing HCI studies have mainly focused on protecting mobile users' privacy by leveraging mobile application analysis [46, 47, 70] rather than sensor data collection for research purposes. In terms of the design approach, these studies have primarily suggested 1) *notice* on privacy-related information to increase privacy awareness, or 2) *control* of data collection permissions based on privacy concerns.

As to *notice*-based designs, the systems aim to deliver diverse privacy-related information to users, such as privacy policy, data flow, and data permissions. Privacy-related data visualization has often been leveraged as a pervasive approach to raise user awareness. For example, Emami et al.'s study proposed a visual representation of privacy policies with the metaphor of the nutrition label to increase users' comprehensibility toward sensor data being collected in IoT devices [19]. HappyPerMi visualizes the data flow of private data collected in mobile applications and informs users how and where the data will be shared [5]. Harbach et al.'s study proposed a system design that offers a preview of private information that becomes accessible when a user installs an app with a certain permission condition [25]. Wilkinson et al.'s design probe varied the granularity and type (i.e., data-centric or app-centric) of visualization to help increase users' understanding of data sharing practices of mobile apps [85].

In terms of *control* of data collection, previous studies often suggested system designs that offer permission control features. A system suggested by Hazim et al. sends nudges to raise privacy awareness and allows permission control (e.g., on/off) of data collection [2]. As part of a privacy nudge that supports user control of their mobile app permissions, Liu et al. [47] devised a Personalized Privacy Assistant (PPA) that recommends the optimal permission configuration based on user preferences. ProtectMyPrivacy (PMP) leverages crowdsourced recommendation to offer app-specific privacy recommendations, which access users' private data and protect user privacy by substituting anonymized data in its place based on users' decision [1].

Sensing platform	Privacy-related features	Reference
CARP	Using built-in privacy data transformation to obfuscate data points when data is collected	[7]
AndWellness	Personal or private information is transferred using end-to-end data encryption	[27]
AWARE	Obfuscate and encrypt data by applying a one-way hashing of logged personal identifiers	[20]
Beiwe	Personal identifiable information undergoes hashing, and all data is encrypted	[74]
Ohmage	Enable to view or delete users' data, change privacy states of users' responses	[72]
HealthOS	Using Key Policy Attribute Based Encryption (KP-ABE) to combine access control and data encryption	[45]
mCelebrum	Using one-way hashing of sensitive data and options to suspend data collection from specific sensors	[28]
ResearchKit	Providing consent in a user-friendly manner	[4]

Table 1: Mobile sensing platforms and their privacy-related features

Since contextual information plays a vital role in privacy decisions, several studies have attempted to consider users' contexts. For example, a large-scale field study with 131 participants was conducted to analyze the contextuality behind user privacy decisions to regulate a mobile app's access to sensitive resources [84]. Similarly, a system design was developed to detect the purpose of privacy-sensitive data access across mobile applications [16]. In attempts to offer a greater sense of user control, the design and implementation of proactive system-driven support have also been introduced. For example, Shih et al. collected users' contexts and measured their privacy preferences in sharing their location and activity information via ESM (Experience Sampling Method) [70]. TurtleGuard learns users' app usage contexts and automatically sets the data collection permission condition (i.e., always/when in use/never) based upon users' decision [78].

Although existing studies have covered the ground in terms of designing usable privacy support, these studies have several limitations: 1) the studies mainly focused on mobile app-specific privacy concerns and decision making with limited data types (e.g., locations, calls/texts), which lacks an in-depth understanding of user perceptions and privacy concerns toward extensive personal data collection in mobile sensing, 2) control features are relatively passive in terms of granting user control, as systems have often provided users with system-driven privacy support (e.g., system recommendation) that lacks proactive user involvement in making informed privacy choices from an early stage of data collection, rendering users to take only partial control of their data, and 3) conventional approaches have often been criticized for abstract or indiscriminate rejections to data collection without sufficient articulation of data collection details (e.g., data types, data collection purpose, data collection status) [11].

2.2.2 Consent Mechanism for User Privacy in Mobile Sensing Research. While data collection and sharing practices are likely to expand as mobile/wearable sensor-enabled research and applications increase, improving existing limitations of user privacy support from previous studies and exploring design opportunities that might better support users' privacy decision-making under mobile sensing contexts seem imperative. Given that users are often inattentive to risk communication due to a lack of transparency in mobile sensing research and limited knowledge in sensor data collection [40], there has been a call for an early intervention that empowers users with easy-to-understand data representations along with transparent instructions to help users make proactive informed decisions [40, 41].

Based on such research needs, improving and developing consent has been suggested as one solution that brings more transparency and grants more user autonomy in mobile sensing studies [49]. Current consent practice in pervasive computing for research assumes participant consent for data collection only at the initial stage [49, 50]. However, given the range of personal data accessible from mobile devices for health-related research, such practice seems to fall short of providing granular control that enables selective data collection/disclosure based on a user's needs or preferences (e.g., disabling GPS data collection when visiting private places) [41, 42].

As the EU's General Data Protection Regulation (GDPR) requires specific descriptions of collected data and its purposes, along with providing participants an option to consent on a granular level across the data collection cycle (e.g., consent (or not) separately to each new data collection) [63], we consider our attempts to explore the feasibility of a more usable and flexible consent mechanism as a timely opportunity.

To better reflect the dynamic nature of mobile sensing, a type of consent called *dynamic consent* was introduced to recent ubiquitous computing studies. Dynamic consent is a type of informed consent that has been originally discussed within the realm of biomedical research [15, 33]. Due to the research community's large-scale and long-term participant engagement for continuous data collection (e.g., biosamples and patient health records), the concept was envisioned to support continuous, bi-directional, and interactive communication between researchers and data providers (i.e., patients) via digital platforms [33, 42]. The crux of dynamic consent lies in its transparency, as it enables interactive communication between the participants and the system to help participants exercise their full rights to their data by offering detailed explanations of data collection and enabling participants to give/revoke their consent to new projects or alter their consent preferences (e.g., access to data, selective data collection/disclosure) along the whole research cycle (e.g., data collection and sharing) [15].

From our knowledge, only a few studies have explored the applicability of dynamic consent in pervasive sensing scenarios, and we deem these studies to be in the very initial stage. According to Lee et al.'s scoping review on dynamic consent for pervasive health research [42], only one study was directly related to the healthcare context. In contrast, the other studies were rather related to discussions on the feasibility of dynamic consent in pervasive computing.

Borrowing the key ideas of dynamic consent, we aimed to design a system that supports fine-grained consent in the context of 24/7 mobile sensor data collection. The system supports the visualization of collected data (i.e., data exploration), and users can dynamically allow or withdraw the permissions of the sensor data collection in a fine-grained manner (i.e., contextual filter). With our approach, we aim to study how a behavior intervention system that leverages data exploration and contextual filter-based design can bring more transparency regarding mobile sensor data collection and guide users to raise privacy awareness. Toward these goals, we set the following research questions:

- RQ1: What are the user perceptions and perceived usability of the PriviAware system?
- RQ2: Does PriviAware positively affect participants' privacy awareness, and how do data exploration and contextual filtering influence participants' behavior?

3 FORMATIVE STUDY

3.1 Method

We began with a formative study to understand privacy concerns of mobile data collection and identify design requirements of systems for user privacy in mobile sensing research. We recruited seven participants (Female: 3, age: M = 24.429, SD = 3.017) via the online campus community board and Facebook. The formative study consists of an online survey and focus group interview. Before the formative study, we introduced the overview of the research (e.g., research goal, data collection). As a first step, participants were given a data sensitivity survey (see Table 2) that provided descriptions of sixteen types of mobile sensor data that will be collected through a mobile sensing platform in the user study [39], and they were asked to rate their perceived level of comfort toward collecting each data type (7-point Likert scale, 1: Highly Negative - 7: Highly Positive, and N/A or don't know). For the questionnaire, we utilized the data sensitivity survey by referencing a prior study that measured the perceived sensitivity of these data collection [40]. The survey was performed to identify which data types are generally considered privacy-sensitive among participants and also to figure out whether the sensitivity level aligns with findings from previous studies on users' privacy concerns in mobile sensor data collection [32, 40, 41]. After the survey, a focus group interview was conducted to support the findings from the survey. During the interview, participants were asked to discuss the following topics: 1) privacy-sensitive data types and contexts on mobile data collection and 2) system design expectations for user privacy in mobile sensing research. Regarding the second topic, participants were asked to draw how they wished data types represented and other desired features that would help explore the collected data. Participants explained and exchanged their thoughts on ideal design features based on the drawings. The interviews were recorded upon participants' consent, and participants' responses were transcribed for thematic analysis. In the following, we detail the major findings of the survey and focus group interview. (Details of the survey questionnaire and interview questions are included in supplementary materials.)

3.2 Result

3.2.1 Data types and contexts. From both the survey and the interview, participants rated high levels of data sensitivity toward the following: *GPS*, *app usage activity*, *call logs*, *app notifications*, *texts messages*, and *camera events*. The most often-cited data type was GPS. Participants were concerned that researchers might conjecture their current status and whereabouts regarding GPS. P3 mentioned, "*It is difficult to know how often and where I meet my girlfriend, but if my girlfriend joins the same experiment, such information can be retrieved from clustering.*" In terms of app usage and app notification, participants were worried that researchers could deduce the characteristics of app usage activities as the name and usage history enable its inference; for example, P2 noted, "*If I always play games, researchers might judge me as a person who always plays games, and I hate it if they accuse me of playing games whenever I do not work hard.*" Moreover, participants considered call logs and text messages as a potential indicator of their interpersonal relationships and social skills, although the collected data are encrypted and only include meta-level information (e.g., number of phone calls/text messages). P4 said, "*The researchers will somehow know how much social impact I have and my interpersonal relationship from my call logs and text logs.*" Additionally, the trustworthiness of the research team also affected participants' privacy concerns. They were doubtful and wished to confirm if researchers stick to IRB regarding data collection and processing. As an example, P7 noted camera event data: "*The IRB document stated that only event types and timestamps are recorded, not actual pictures taken. However, I'm not sure if the researchers do follow that principle.*"

In terms of contexts, participants recalled privacy-sensitive contexts (e.g., time and location) in their daily lives. Reported privacy-sensitive contexts varied significantly based on their social settings. For example, participants generally wished for a pause in data collection during nighttime at home as they considered the context private. One interesting comment from a participant was that he would intentionally change his persona depending on public/private settings so that he is mindful of using his smartphone in public contexts. P6 commented, "*I think I'm a different person when I'm just by myself or surrounded by others. That also affects how I use my phone. For example, what types of apps I would use during the daytime with others and what I would browse through during the night when I'm just by myself would be different.*"

3.2.2 Design expectations. Based on their privacy concerns, participants suggested several design expectations. Participants desired to check how mobile sensor data was collected to clarify their privacy awareness. Although detailed descriptions and lists of data types were provided to participants, they still had curiosity and privacy concerns toward data collection. To understand collected data intuitively, they suggested several visualization supports with drawings (Fig 1). Rather than checking all log data in a tabular format, they preferred aggregated information with a graphical representation.

Data type	Description	Mean	Median	SD
GPS	Location change (GPS signals)	1.43	1.00	0.49
App Usage Activity	Installed app list and app use history	2.29	1.00	1.75
Phone Calls	Call history (with encrypted contact number)	3.00	3.00	1.15
App Notification	App notifications at notification bar	3.57	3.00	1.76
Text Message	SMS/MMS history (with encrypted contact number)	3.71	4.00	1.67
Camera Event	Type (picture/video), time of record	4.29	4.00	1.03
Wifi	Nearby wireless signals (e.g., SSID, SNR)	4.43	5.00	2.26
Activity State	Physical activity (run/walk/in-vehicle/...)	4.86	5.00	1.64
Key Distance	Grid length, the time interval between input keys	5.14	5.00	0.99
Input Key Type	Character type (Korean/English/special/etc.)	5.43	6.00	1.50
Keyboard Type	Korean keyboard (chun-ji-in/qwerty/etc.)	5.43	6.00	1.50
Network Usage Data	Network usage (Tx: transmitter, Rx: receiver)	5.57	6.00	1.29
Power Status	Power on/off, screen on/off	6.00	6.00	0.94
Ringer Mode	Normal/vibrate/silent	6.14	6.00	0.35
Charging State	Charging/discharging	6.14	6.00	0.64
Battery Level	Level of battery remained	6.29	6.00	0.40

Table 2: Privacy sensitivity score toward mobile data collection (1: Highly Negative, 7: Highly Positive)

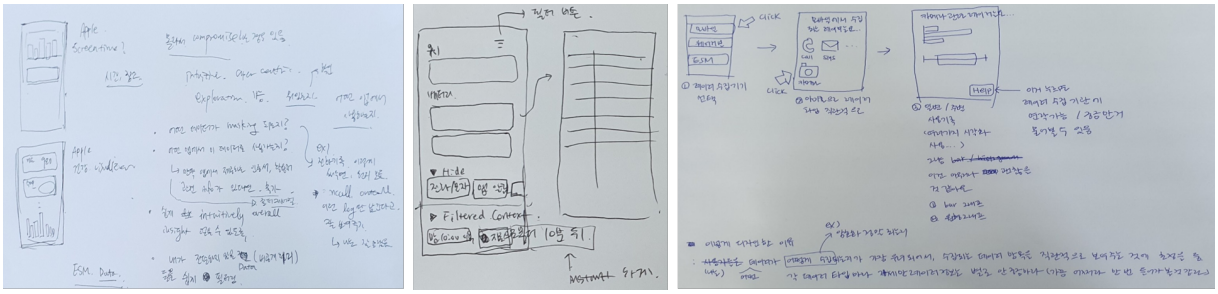

Figure 1: Drawings from focus group interview about visualization support. Participants suggested several visualization supports such as a bar graph (left), sensor data lists (middle), and icons with detailed explanations of each sensor data (right)

According to the sensor-specific data types (e.g., numerical, categorical, etc.), they draw diverse graphical representations to check the aggregated data. For example, P1 illustrates an example of app usage activity data: "*I want to check when and what types of app I used with these bar charts, rather than checking all detailed logs. I think the summarized information is enough.*" On the other hand, some participants wanted to see detailed data logs to secure their trust in the research team. P7 stressed, "*The most important thing for me is whether the research team encrypted or anonymized data as specified in the IRB documents. Therefore, I want to check some of the raw data logs.*

Furthermore, participants wanted to be able to control data collection for privacy-sensitive contexts by themselves. Their privacy concerns are greatly affected by time and place, so they wanted to pause data collection if they were in a specific place or time range. P5 mentioned, "*I think it would be nice to remove the data when I am in my home or to remove the data during nighttime.*" Adding to this, P3 suggested adding on/off switches so that he can freely control the context of data collection: "*I want to make sure that GPS data is collected only when I'm in a public context. It would be good to turn on them from 9 AM to 6 PM, my working time.*"

4 SYSTEM DESIGN

4.1 Method

To design and implement the system, we conducted three iterations of prototyping. Three researchers conducted paper prototyping of the initial design based on the formative study results. We invited two graduate students with rich interface design experience and explained our initial prototype. We described the reason behind the design by introducing the significant findings in the focus group interviews. They provided their opinions about whether the initial prototype aligned with the participant's expectations and

design suggestions. Especially for the data exploration feature, we summed participants' drawings according to data types (e.g., numerical, categorical, geographical). They discussed the advantages and disadvantages of the proposed graphical representations for each data type, finally making a consensus on the most suitable one. After collecting feedback for improvement, we implemented a mobile application as the second prototype. To explore its feasibility and usability in an in-the-wild data collection environment, we conducted a pilot test with nine students (5 female; age: M = 24.43, SD = 3.02). They installed the mobile application on their smartphones, tested them for one week, and provided feedback regarding usability issues and design improvements. Finally, three of the authors summed up the feedback and implemented a final system, *PriviAware*. In the following, we describe the design components of the system with major changes that occurred during the prototyping process.

4.2 PriviAware System

PriviAware is a mobile intervention app for promoting participants' proactive data collection consent and privacy management in a mobile data collection environment (Fig 2). Based on the formative study results, we set up two design goals for the system. First, participants wanted to understand how their mobile sensor data was collected to be aware of the privacy concerns regarding data collection. Thus, the system provides visualization support tailored to each sensor data type to raise privacy awareness. Second, they desired to control the permission of privacy-sensitive data collection contexts, such as specific times or locations. Our system enables users to pause sensor data collection according to user-defined filtering contexts, termed as *contextual filtering*. Users have two options for setting the filtering conditions: they can entirely switch on/off specific sensor data collection, or conditionally switch on/off according to time and location.

Whenever users have potential privacy concerns, they can open the app and sign in (Fig. 2a) and overview mobile data collection status (Fig. 2b). To explore the privacy-sensitive data types with higher priority, the system groups and displays six sensitive data types (e.g., app usage history, phone calls, GPS, camera event, text messages, and app notification) on the upper part of the page. Two dots for each row correspond to two types of contextual filtering: 1) entirely on/off of specific sensors (left dot; purple as on and gray as off) and 2) conditional on/off based on time and location (right dot; purple as on and gray as off). Clicking the help icon ("?" icon) for each row shows a description of the data type and contact information of the researchers who can access the data so that users can easily communicate with researchers when they have privacy concerns regarding data collection (Fig. 2c).

Sensor data exploration for raising privacy awareness toward mobile data collection PriviAware provides a graphical representation according to each sensor data. When the users choose specific sensor data types in Fig. 2b, the system supports visualization of the selected data (Fig. 2d, Fig. 2e, Fig. 2f). Specific dates and hours for data exploration can be selected on the 'Date' and 'Hour' pickers on the upper part of the page. The system provides different graphical representations that can adequately show each type of data: categorical data as a stacked bar chart (x-axis as hour, y-axis as the number of rows, and the color encoding as type of each category), numerical data as line chart (x-axis as hour, y-axis as data values), and geographical data as map representations. Fig. 2d, Fig. 2e and Fig. 2f represent the examples of app usage history along time and types of data, battery level along time, and GPS logs on a map, respectively. Not only for the graphical representation with aggregated information, the system also provides examples of detailed data logs to ensure that the data is properly anonymized and encrypted. When users tab the graphs, it shows the first five rows of the collected data (Fig. 2g). While prototyping the graphical representations, we first considered using unified bar charts for all sensor data types; however, it was improved to the three types of graphs reflecting the feedback from the first prototyping session.

Contextual filtering for fine-grained permission control toward mobile data collection Based on insights obtained from sensor data exploration, users can set filtering conditions for data collection according to their privacy concerns. In a way that can completely restrict a certain type of sensor data collection, the system provides a full on/off feature of a sensor data type (upper-right toggle button in Fig. 2d, Fig. 2e and Fig. 2f). However, switching off a specific sensor can lead to a complete data loss for research, so the system also supports a feature that allows users to pause data collection only in privacy-sensitive contexts (e.g., time and location). Pressing the 'New filter' button in Fig. 2d enables users to make a new contextual filter (Fig. 2h). For the specific period to pause data collection, users can turn on the 'Time' toggle button and set the period for filtering (e.g., do not collect my data from 7 PM to 10 PM). In addition, they can turn on the 'Location' toggle button and pin the specific location to pause data collection with radius (e.g., do not collect my data within 150m of this pin). After setting filtering conditions and tapping the 'add' button, a filtering condition is added. According to users' conditions, data filtering (e.g., data deletion) is conducted periodically daily. The filtering query is logged and applied to the database every day at 2 AM; then, the data is deleted according to the contextual filtering queries. In the initial prototype, the filtering condition was designed to set only one for a sensor; however, the system was improved to set multiple filtering conditions by reflecting feedback from pilot test participants.

To secure the reliability and validity of data exploration and contextual filtering features, we went through a one-week pilot test to assess the system's operation against our expectations. We verified that the collected data was correctly visualized on the system through manual downloads and plotting of raw data from the database. We also checked that setting the contextual filtering conditions is logged as query data; then, the queries were applied to delete the raw data at a predefined time.

5 USER STUDY METHOD

We conducted a user study by deploying the PriviAware system in an in-the-wild mobile sensor data collection environment for three weeks. The main goal of our research is to investigate 1) the perceived usability of the PriviAware system and 2) the effectiveness of the PriviAware system on users' privacy perception. To achieve the second goal, we designed the study as follows.

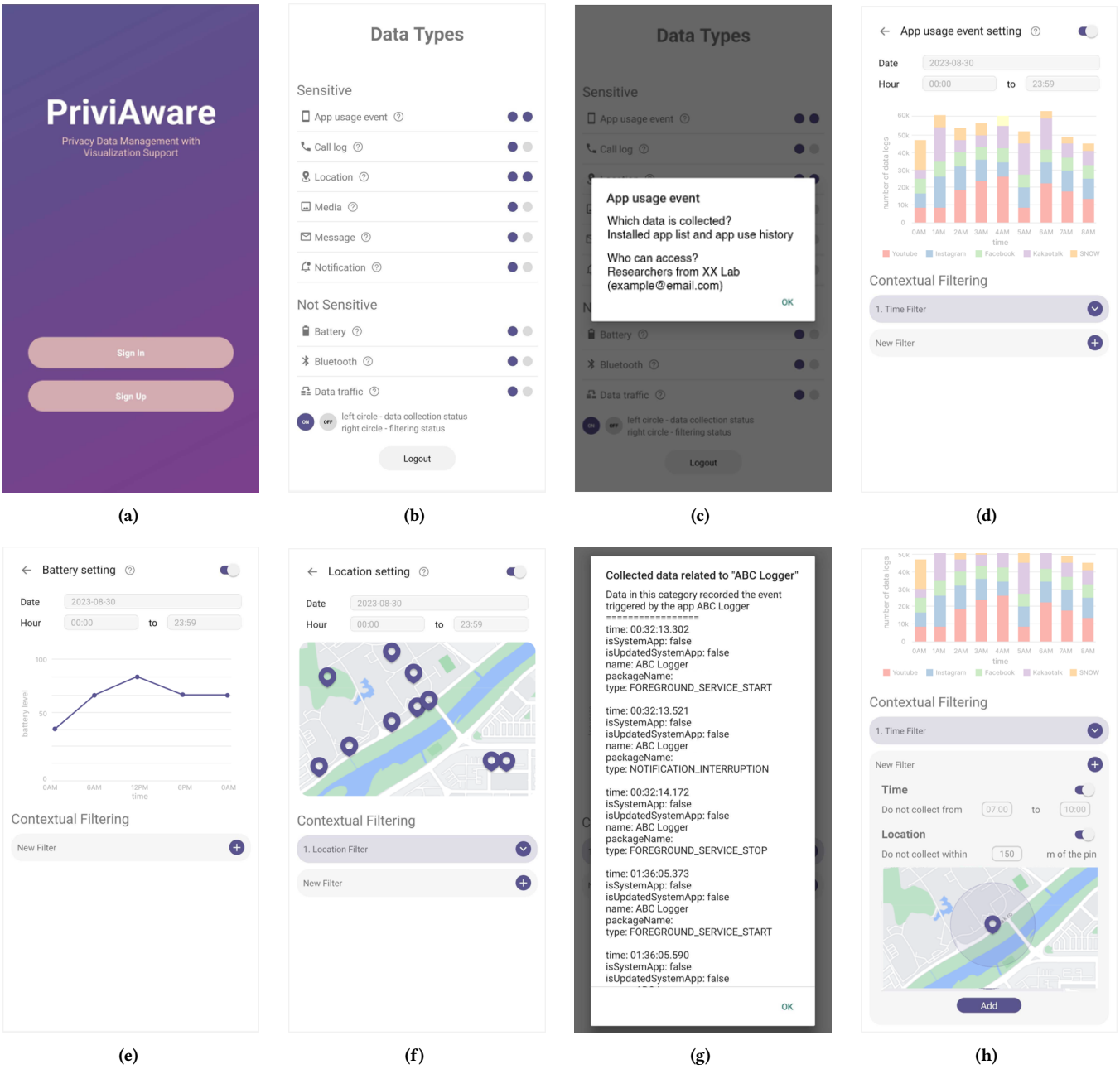

Figure 2: Major screenshots of PriviAware system. Starting from the upper left side, four images are about (a) Intro page of PriviAware app (b) data type list page (c) popup for help button (d) visualization support for categorical data, and starting from the lower left side contains images of (e) visualization support for numerical data (f) visualization support for geographical data (g) popup for raw data example (h) contextual filtering setting

5.1 Study Design

Fig 3 describes the overall study design and procedure. We chose a mixed design experiment (e.g., a mix of both between- and within-subject factors) to analyze the effect of the PriviAware system on the perceived level of privacy concerns and awareness. As the between-subject factor, we chose contextual filtering. We initially considered the comparison between conditions 1) without the PriviAware and 2) with the PriviAware (containing both data exploration and contextual filtering). However, we postulated that this approach can result in the mixed effect of two features (i.e., comparing two conditions includes the mixed impact of data exploration and contextual filtering). Therefore, we divided the conditions into 1) PriviAware

only with data exploration and 2) PriviAware with both data exploration and contextual filtering to explore how contextual filtering comes into play when it is combined with data exploration (i.e., visualization), which has been a well-known method for effective delivery of privacy information to users [3, 10, 12]. We divided the participants into Group A and Group B and provided the first and second conditions of PriviAware, respectively. The within-subject factor is time (especially for the week); we aimed to identify how participants' privacy concerns and awareness evolve as they transition from not using the system to using it. The dependent variable is the perceived privacy concerns and awareness, and we quantified the score based on the survey used in the prior study [40]. In the survey, participants rated 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). The survey items were derived from prior studies in biomedical research [54, 56, 69] and a widely-used scale from the field of information science [48, 87, 88]. The survey items are described in the following and detailed in supplementary materials.

- Demographics: Participants' age, gender, education
- Confidence in knowledge: Participants' self-assessed confidence and interest in their knowledge of the research context (e.g., mobile 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)
- Risk-benefit assessment of open dataset collection: Participants' attitudes toward perceived risks (e.g., privacy threats) and benefits (e.g., scientific contribution) [56, 69]
- 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 mobile dataset collection and public release ([87, 88])
- Level of trust: Participants' assessment of their level of researchers and overall research process (e.g., data processing) ([48])

5.2 Participants

We recruited 58 participants (26 female, age: M = 22.59, SD = 4.19) from an online campus community board and Facebook. Participants consist of 30 undergraduate students, five graduate students, and 23 non-students. Except for one participant with rich experience in sensor data collection, other participants do not have sufficient background knowledge in mobile sensor data collection. Reflecting the prior studies conducted between-subject controlled experiments [9, 43], we aimed to recruit at least 20 participants for each group.

5.3 Procedure

As illustrated in Fig 3, the user study was conducted for three weeks consisting of a one-week baseline period and two weeks of the intervention period. The study period was determined by reflecting on prior HCI studies [36], which aimed to compare the baseline and the intervention period. At the beginning of the study, participants took an online orientation with consent in IRB documents. The orientation included the goal of the study, types of mobile sensor data collected, an explanation of the PriviAware system, and tasks that participants should complete during the experiment. As to the purpose of data collection, we described to our participants that it is essential to collect vast amounts of mobile sensor data in the context of mobile health research (such as stress detection and mood inference). Since the participants were unfamiliar with the mobile sensor data collection environment, they had the first week as the baseline period to experience the context. They installed a mobile sensor data collection application (ABC Logger [32]) on their smartphone. The application collects mobile sensor data, such as location, proximity sensor readings, and app usage history.

At the end of the first week, participants completed the survey questionnaires mentioned above. To ensure that both groups' privacy concerns are unbiased, we adopted a stratified sampling [58] when assigning participants to Groups A and B. We averaged the survey score for each participant and made two strata based on them: 'high' (the score is higher than 4) and 'low' (the score is lower than 4), assuming that the score 4 represents 'neutral.' The proportion of participants with 'high' and 'low' categories was 35: 23 (approximately 1.5: 1). From the 'high' and 'low' groups, participants were randomly sampled for Group A and B so that each group had the proportion of approximately 1.5: 1. We iterated this process until the average of the score between two groups is not significantly different in t-test (t = .03, p = .48). Finally, Group A has 18 people with 'high' group and 11 people with 'low' group, and Group B has 17 people with 'high' group and 12 people with 'low' group.

We let participants install the PriviAware application on their smartphones for the second and third weeks. The ABC Logger application collects individuals' mobile sensor data and sends them to the database, and the PriviAware application extracts and provides visualization. As mentioned, participants in Groups A and B received the system 1) only with visualization support and 2) visualization support with contextual filtering, respectively. Participants in Group A were instructed to access the app and explore the data at least once a day, depending on their interests. For Group B, they also explored the collected data similar to Group A and set the contextual filtering conditions. When introducing the contextual filtering features to participants in Group B, we explained that the filtering would not delete their data in real-time but delete their data every day at 2 AM and update the result on the system. At the end of the second and third weeks, participants were asked to respond to the questionnaires the same as the first week.

After the experiment, we conducted a semi-structured follow-up interview with 20 participants (6 female; age: M = 23.06, SD = 2.88; 10 people for each group). We asked 1) their perception toward the system and the perceived usability, 2) how their privacy concerns and awareness were changed after using the PriviAware, and 3) their further expectation toward a user-friendly privacy management system. The interview was conducted online for 40 minutes, and all contents were recorded and transcribed after getting participants' consent. As compensation for the three-week participation, they received 75 USD (an additional 7 USD for the follow-up interview). The Institutional Review Board (IRB) approved the whole study process and obtained written consent from participants.

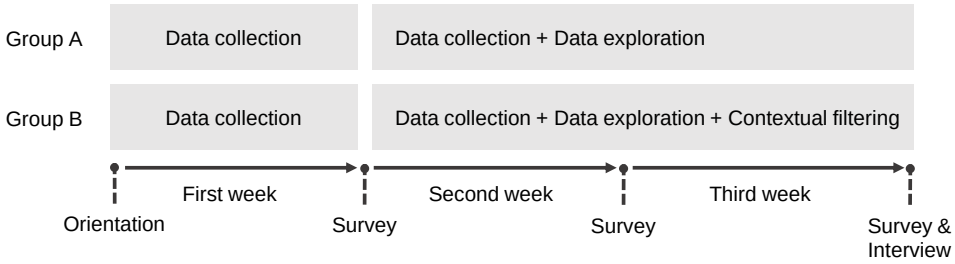

Figure 3: Study design and procedure. For the first week, which is a baseline period, both Group A and Group B allowed data collection from ABC Logger. Following two weeks of intervention with PriviAware system, two groups were treated differently with different conditions. For Group A, their data was collected via ABC Logger, and they were asked to explore their data with the data exploration feature only. For Group B, their data was collected via ABC Logger, and they were asked to explore their data with the data exploration feature and contextual filtering to alter their data collection consent based on time and place as they wished

To analyze the transcribed interview dataset, we performed thematic analysis [14] consisting of six stages: familiarization with the data, generating codes, searching for themes, reviewing themes, defining and naming themes, and producing the report. Following the process, two researchers reviewed raw transcribed data, assigned thematic codes, and prioritized similar themes depending on the frequency of codes. They repeated the process until they reached a consensus.

6 RESULTS

In this section, we report the qualitative analysis of the semi-structured interview and the quantitative analysis of the survey result. Through this process, we explored how participants perceived the design components of the PriviAware system and changed their privacy perception toward mobile sensor data collection. Table 3 shows our research questions and the summary of major findings.

6.1 User Perception and Perceived Usability of PriviAware (RQ1)

We present our findings on participants' perception and perceived usability of two representative features of the PriviAware system: 1) data exploration and 2) contextual filtering. For system evaluations, we inquired about their utilization of design components of the PriviAware system and assessed its perceived usability. Overall, participants provided positive responses in the SUS (System Usability Scale) questionnaire; the average score in Group A was 73.3 (SD = 13.06) and in Group B was 73.1 (SD = 7.52), which can be interpreted as 'good' system usability [6] (the scores range from 0 to 100). Here, we denote the participants from Group A as "Ak" and participants from Group B as "Bk" (k = participant number).

Data exploration All participants perceived that the visualization support provided by the PriviAware system was an intuitive way to represent mobile sensor data. For example, B1 remarked, "*All the graphs shown in the app were easy to understand, and nothing posed any difficulty.*" They thought that the different graphical representations according to data types (e.g., stacked bar graph as categorical data, line graph as numerical data, map representation as geographical data) were properly selected, considering the characteristics of data types. A8 pointed out, "*I think the biggest advantage of this visualization was that I could see a graph tailored to each data type. Bar graphs, line graphs, and maps were all appropriate choices for each data.*" Expanding upon the current visualization, six participants proposed several improvements to the graphical representations to facilitate a better understanding of the collected data. In particular, they pointed out the stacked bar graph and map representation. As the number of categories in the data increased, the stacked bar chart became more complicated to interpret. For example, A6 stated on app usage data: "*The categories within a bar were quite diverse because I use many apps on my smartphone. It might be beneficial to arrange them in order of the most frequently used apps while grouping some less significant categories as 'others' categories.*" As to map representation, A9 reflected the cases when the number of pins on the map increased: "*All the places I visited were marked with pins, but in such cases, many pins overlapped, making it difficult to distinguish each pin. It would be advantageous to delete a few overlapping ones or display only the locations I visited frequently.*"

Contextual filter Overall, participants found it straightforward to establish filtering criteria based on their privacy-sensitive times and locations. B10 stated, "*I could customize these conditions according to my preferences. Right? It was intuitive to configure various filtering conditions within the app.*" They initially explored the collected data through graphs, identified specific contexts to filter, and set those filtering conditions on the 'contextual filtering' panel. Despite its ease of use, participants desired to enhance the time filtering feature. In the current filtering setup, when users specify a period to filter, data is deleted that night; therefore, checking whether their data was filtered immediately as expected was challenging. B1 commented, "*When I set the filtering conditions and pressed the 'add' button, I could not verify whether my data would be deleted. To ensure that my input is properly applied, I wish the system would indicate which data will be removed when I apply the filtering conditions.*."

RQ1. What are the user perceptions and perceived usability of the PriviAware system?
• Participants perceived data exploration and contextual filtering features were intuitive and easy to use, with suggesting improvements for graphical representation and interactive features
RQ2. Does PriviAware have positive effects on participants' privacy awareness and how do data exploration and contextual filtering influence participants' behavior?
• The comparative analysis showed the score of the privacy awareness had significant increases over weeks, but did not have significant differences between groups • Group A, employing only data exploration, could raise their privacy awareness, particularly regarding sensitive data types, and also self-reflect their daily lives • Group B, employing data exploration and contextual filtering, similarly exhibited heightened privacy awareness, additionally experiencing *a sense of empowerment* in controlling data collection based on contextual filtering

Table 3: Summary of qualitative and quantitative findings according to research questions

6.2 Effectiveness of Intervention (RQ2)

Overall, participants from both groups responded that their privacy concerns and awareness increased over time compared to the baseline period. Here, we elaborate on how PriviAware affected users' privacy perception and usage of intervention features (data exploration, contextual filtering).

As noted earlier, we handed out survey questionnaires on participants' perceived level of privacy concern and awareness in sensor data collection at the end of each week. To further explore how PriviAware influences participants' perceptions of privacy awareness, we statistically compared participants' responses according to weeks (1st week vs. 2nd week vs. 3rd week) and groups (Group A vs. Group B). For the comparative analyses, we ran a Mann-Whitney test to figure out differences in survey scores between groups and a Kruskal-Wallis test to investigate differences in survey scores between weeks. Our results showed no significant effect of groups and weeks in the survey scores. Even though the comparative analyses did not show a significant effect according to groups and weeks, we could identify how our systems affected participants' privacy awareness through the follow-up interview. In particular, although there was no significant effect of privacy awareness according to groups, we identified meaningful insights when contextual filtering was adopted in the system. In the following, we explain the detailed experiences of each group in PriviAware usage.

6.2.1 Group A: Data exploration. Here, we describe the user experience and privacy perceptions of participants from Group A, who only used the data exploration feature.

Changes in privacy concerns and awareness. Group A, supported only with data exploration, generally reported that visualized representation of collected data with supporting descriptions helped them gain better insights into their data and raise their privacy awareness. For example, A1 commented, "*I was kind of hopeless whenever I thought about my data. We all know that our data is everywhere these days without our consent. That's probably why my score for privacy concerns was pretty low in the beginning. But now that I can look at my data with these graphs and maps…I think I became more aware of how my data is being collected.*" A2 added, "*I think there's a big gap between just knowing and knowing upon seeing visible data. I just had a vague idea of smartphone data collection because you don't know what's happening once you consent. It's like putting all your data into a black box. But this app is transparent, I guess. It lets you view your data with easy-to-understand support, so it's different from when I just gave up on privacy because I didn't know anything.*". One participant reported increased privacy concerns as PriviAware unintentionally provided a sense of surveillance due to its informative characteristics in the data exploration feature. A4 noted, "*I don't consider smartphone data a critical threat to my privacy. If it were directly related to my medical records, I would've been really sensitive. Even with the PriviAware installation, I wasn't concerned that much. However, after one week of intervention, it occurred to me that this app shows every footage of me. I'm being monitored! (laughs)' Since then, I felt extremely uncomfortable that my smartphone is more dangerous than I think.*"

One interesting thing to note about data exploration is that it played as a double-edged sword to participants. While most participants reported increased privacy awareness as they viewed data exploration as a mirror reflecting their digital footprints, ironically, some participants reported relief as they were constantly provided with transparent footage of their data. For example, A5 mentioned, "*It might sound weird, but I was rather unconcerned after the experiment. Of course, I was surprised to find out that much of my data is being monitored and collected. But if you look on the bright side, it's better to be exposed to the truth than not knowing anything (laughs). I got used to data exploration for two weeks, and as I inspected my data, I came to think, 'Well, there's not much data that is so revealing. I think I'll be okay.'*" Similarly, A9 reported, "*For the first few days into the intervention, I felt repulsed because my data was being shared with you guys. However, as I constantly checked my data with the data exploration, I felt it was helping me be conscious of my rights to protect personal data. Since I could check my data at any time and find out what data types were being collected, I felt rather safe. That's probably why my privacy concerns decreased.*"

Data types and contexts. Participants' perceived sensitive data types centered around GPS, call logs, and app usage. A1 commented, "*I only explored my location data. There is a lot of heinous crime news*

these days, and I'm scared. I've heard that criminals often keep track of a victim's location traces." A6 added, "*I used to be okay with GPS data because I often allow location data to be collected and shared for other service applications. In this experiment, however, I was quite surprised to see that I was able to view accurate traces that include not just the current location but my past whereabouts. You can even check longitude, latitude, and altitude. That's too much."* A7 noted, "*I was concerned about my GPS and call logs. If you carefully look at the visualized representations of these data daily, I think others can grasp my daily life. I tried to behave differently or act cautiously to hide private parts of my data."* A8 mentioned app usage as a sensitive data type, saying, "*I often stay up late at night and browse through different apps. If you combine the types of apps I often use with WiFi data; you can infer how much I use a certain app. Then, you can naturally guess my lifestyle and preferences, right?"*

When asked to recall specific contexts in which participants explored their data using PriviAware, we found that responses did not significantly differ. We posit that this is due to similarity in participant demographics, whose daily activities and social interactions occur mostly within the campus. Some participants responded that their lives are too mundane to extract special patterns that can identify them, thinking other participants' data would look similar. However, one interesting thing to note is that participants would rather take data exploration as a daily routine. Instead of looking at and interpreting their data in specific contexts, many participants responded that data exploration became a daily routine during the experiment. For example, A2 said, "*I think I explored my data whenever I had free time."* A8 added, "*I think it's hard to talk about certain sensitive contexts regarding time and place. I think I checked my data in my dorm room at the end of the day. You know, you wrap up your day by reflecting upon all the private data collected daily. It's like a daily ritual."*

6.2.2 Group B: Data exploration + Contextual filter. In the following, we detail the experiences and privacy perceptions of participants in Group B, who leveraged both data exploration and contextual filtering.

Changes in privacy concerns and awareness. Group B was provided with both data exploration and contextual filter, which allows participants selective data collection consent based on their contextual (i.e., time/place) preferences. Compared to the baseline period, most of the participants from Group B also reported an increase in perceived privacy concerns and awareness due to the data exploration feature. For example, B2 noted, "*I'm generally very concerned about my privacy. Recently, I've watched a lot of movies about personal data abuse. But the truth is I didn't clearly understand what types of sensor data could be collected from my smartphone. From the visual representations of data, I was quite surprised to see how much personal information could be inferred from the smartphone data and to what extent it is possible to make a detailed profiling of a person. Since I joined the experiment, I'm worried more than ever."* B1, who called himself tech-savvy, would report, "*My research area deals with mobile sensor data collection and its processing. I would often become curious about data collection, but there was no tool for me to explore. So, what I did was look into each file and go through the text data. But now, with this app, that process has become much simpler. Plus, you can view the sensitive data that turns into graphs immediately (laughs). You can see the pattern; thus, I think I became more aware of my data."*

Although participants generally reported similar tendencies regarding privacy concerns and awareness, participants from Group B expressed a greater *sense of empowerment* as they were allowed to turn off data collection upon their decision proactively. B8 mentioned, "*I think it's really interesting… Once I explored my data, I was concerned that so much of the data was collected. But since I can filter data collection that occurs during the time while I am at a certain place, I think I was instantly relieved and empowered (laughs)."* B4 similarly commented, "*Data exploration feature alone is already beneficial. Adding a contextual filter gives people a sense of psychological safety because you get to be the driver of your data collection."*

While this empowerment generally had a positive impact that led to participants' increased privacy awareness and attempted to use the contextual filter for their data protection responsibly, the presence of the feature had a reverse effect on a few participants. For example, B10 noted, "*I think contextual filter got rid of all my existing privacy concerns. The fact that I could set up a rule at any time just for myself made me feel like I had full control. It's ironic, but that's why I didn't use the filter that much."* We posit that such responses may be due to the "control paradox." According to the term, people are likely to underestimate the potential privacy threats and become more generous toward their data being collected and shared due to their misconception regarding data control [13].

Data types and contexts. Regarding data types and contexts, participants from Group B reported a more active user experience with PriviAware as they were provided with the additional feature (i.e., contextual filter). B4 said, "*I think I set the location filter on my GPS data whenever I was outside the campus. I'm pretty sure most of the participants' location traces would look similar within the campus, but once I'm out, it's a different story."* B6 added, "*Honestly, I didn't care initially. However, as I did my data exploration, I found that collecting private data such as location or app notifications is especially clustered around after midnight. After that, I actively set both a time and location filter. I think choosing to use just one filter is not enough. First, I would set the time filter on any irregular data collection outside my routine. Then, I would make granular adjustments with the location filter. It was really helpful."* B5 noted, "*I think app usage and notifications are the strongest predictors of identifying someone. Based on a certain email application or game app that I use, it's easy to outline my characteristics. I don't really use those kinds of apps during the daytime because I have to take lectures. Thus, I would set the time and location filter on app usage and notifications at night or any private moment I encountered during the experiment. Having to set up a filter every time was a tiring process. Still, I intentionally did it anyway because I felt the research team could take away every personal detail about me."* B8 showed very sensitive responses to his social interactions being monitored. He commented, "*From 9 to 6, most of the calls are related to work, so I didn't set any filter. After that, however, I actively set time and location filters on my call logs because I go to the gym and do many social gatherings outside. Sometimes I forgot to set up a filter and was so upset (laughs)."*

7 DISCUSSION

This exploratory study aimed to investigate the overall user experience of the PriviAware system and explore how different conditions (Group A: Data exploration, Group B: Data exploration + Contextual filter) affect participants' behavior. We summarize major findings by discussing the effectiveness of the proposed data exploration and contextual filtering to raise participants' privacy awareness. In addition, we provide practical privacy-by-design guidelines to support user-centered consent for mobile sensor data collection.

7.1 Promoting Privacy Awareness in Mobile Sensing

Our experimental results showed that data exploration with visualization support and contextual filters helped participants become more aware of their data and consciously adjust their data collection consent. In terms of data exploration, it was found to be intuitive and informative and served as a self-reflection tool that helped participants reflect on their daily routine and relevant private data. Participants from both groups reported that visualized representations of the collected data helped them realize how much and to what granularity of sensor data can be acquired from an individual within a day. The alarming nature of data exploration made participants more aware of their data and potential privacy issues. In contrast, a few participants were less concerned and somewhat relieved to see the actual footage of the collected data transparently. Interestingly, both sides made such ambivalent responses since they considered visualization support much more helpful than having a vague concept of sensor data collection without any visible information. This finding aligns with previous research on the effectiveness of data visualization support for personal data collection. Numerous studies that leverage ex-post visualization tools [3, 21], which focus on showing users types of data collected and how those data have been shared since a user started using an application, have demonstrated that visualizations have two key advantages when it comes to representing privacy-related information; *expressiveness* and *engagement* [24]. The specified uses of data and engaging experience provided by graphical representations that rarely bother participants to read through the text made participants actively involved in the data exploration process.

Although our comparative analyses reported no statistical significance regarding group differences, our in-depth interview showed that contextual filters supported a relatively greater level of participants' engagement. Given an opportunity to leverage fine-grained control on a wide array of sensor data, participants from Group B expressed a greater sense of empowerment as they could set up a rule based on their contextual needs. One interesting behavioral pattern observed from participants' responses in Group B is that they were generally carefree initially, started data exploration, and moved on to actively use contextual filters out of increased privacy concerns and awareness. Participants would use data exploration as a self-reflection tool and make two kinds of contextual filtering based on the reflection: 1) regular filtering for daily contexts and 2) one-time filtering for special occasions. From this observation, we find that combining data exploration and contextual filters amplifies participants' privacy awareness and guides them to continuously observe and configure their data collection settings in various contexts. Our synergetic design approach builds upon existing usable data collection consent mechanisms that provide mere on/off features [2, 41], suggesting a novel design dimension that offers more flexible and context-aware intervention for participants' privacy in mobile sensor data collection.

Besides the aforementioned two primary features, we informed both groups that they could fully enable or turn off data collection (i.e., entirely on/off feature) as they wished. However, none of the participants reported using this feature during the interview. When asked to recall their experiences, many participants viewed entirely turning off data collection as a selfish behavior. Group A participants without a contextual filter allowed complete data collection across the two weeks of intervention. Participants from Group B also reported that they haven't considered entirely switching off the data collection. Though the primary purpose of this research was to explore PriviAware's usability and its effect on participants' privacy awareness and following behaviors, participants from both groups paid considerable attention to data collection. Participants were aware of the significance of data collection for research purposes and thus deemed switching off the whole data collection unethical. Participants were concerned about their privacy, but they were also willing to sacrifice their privacy to a certain extent out of altruistic motives since the data collection was going to be used for research purposes [40]. Aside from altruistic motives, we also posit that participants may have intentionally refrained from entirely switching off as they have been influenced by a behavioral urge to act to live up to the expectations of researchers (i.e., social desirability bias) [23]. From this, we find that there should be further studies on accommodating and balancing the needs and tensions of both data contributors and researchers.

To investigate privacy awareness and concerns for mobile data collection, PriviAware presented numerous lists of sensor data items. However, participants felt exploring all the lists was cumbersome and did not feel the necessity to explore all of them. Their interests were mainly directed towards specific data types like app usage and GPS, which can mirror their personal traits or social behaviors [17, 65]. In contrast, exploring data like Bluetooth or WiFi was perceived as insignificant, contributing to enhancing their privacy awareness. We posit that such contrasting responses may have also been affected by the data granularity presented in the system, while the participants perceived representations of data such as GPS or app usage as highly granular, whereas line graphs that deliver information on data types such as battery or WiFi to be coarse and not containing sufficient information. Our findings imply that focusing on fewer data types closely related to privacy issues and also balancing the data granularity would be more effective in reducing the burden of data exploration and further enhancing the system's usability. Furthermore, future studies should keenly explore participants' perceived sensitivity per data item in relation to different contexts to make more accurate observations on participants' privacy decisions.

7.2 Toward Data-Driven and Automated Intervention

While participants noted that configuring diverse contextual filters supported addressing their privacy concerns, they also found it burdensome to set up a filter every time. This challenge was frequently reported among participants using regular filtering for daily contexts. For example, participants would have a predetermined set of rules in mind but sometimes need to remember to set up a filter. Furthermore, our results showed difficulties in determining which filter (i.e., time, location) to use on which sensor data types, which also caused cognitive load among participants. Such findings align with the implications of existing research that explored the feasibility of dynamic consent in pervasive computing. In the study, participants experienced *decision fatigue*, as they were allowed to review extensive lists of mobile sensor data and manually turn on/off each sensor data in privacy-sensitive contexts [41]. Similarly, participants in our study had to navigate through numerous sensor data items and make decisions regarding contextual filters.

Following this statement, one potential design consideration is introducing data-driven and automated context-aware support based on one's daily routine. Based on the aggregated data of a user, a system can automatically cluster frequently visited places and times (e.g., school: 10 AM - 5 PM), presenting many different default settings [26]. Such categorized selection may lower the burden of turning data collection on or off. Another approach is to envision a rule-based approach (e.g., trigger-action programming). For example, users can set up rules (e.g., turn off data collection) by reflecting on their daily routine instead of repeatedly navigating around a map or time picker and deciding where/when to set the filtering condition [86]. Given the complexity and repetitive nature of data collection consent, providing automated support to users with a data-driven approach will offer flexibility during the intervention. However, a critical dimension to be considered is to what degree such flexibility will be permitted. Thus, choosing the proper defaults in interaction design should be carefully considered in future studies [90].

7.3 Exploring Privacy Nudges for Comprehensive Support

Our results also showed that having to set up a contextual filter on special or urgent occasions (e.g., social gatherings) outside of the daily routine caused participants additional mental costs and giving up on their privacy. One possible design solution is to employ proactive interventions that nudge participants about alarming data collection and offer an option to browse their data [2, 59]. As the most simple way, we can consider periodical alarming (e.g., twice a day) or simple rule-based alarms using trigger-action programming [44, 91] (e.g., if I meet a specific condition, then send me a notification). Extending from the previous section, the system can automatically mine users' routine behavior patterns (e.g., clustering GPS traces) and provide interventions by detecting events when users are in an unusual context (e.g., visiting new locations). For example, it may give a gentle reminder such as: "*It seems that you are in an unusual time and place. If the current context generates privacy-sensitive data, how about setting contextual filters?*" Likewise, providing such nudging can support users in remembering to set filtering conditions, thereby preventing the collection of privacy-sensitive data.

7.4 Limitation and Future Work

We identified several limitations in our study. First, our system design and evaluation may not encompass the perspectives of diverse populations because most of the formative and user studies participants were undergraduates or graduate students. Moreover, some participants' perception that a certain amount of dataset should be contributed for *research purposes* may also have affected the use of the system (e.g., such as setting contextual filtering). We introduced our context of the data collection as the research purposes in the mobile sensing research domain, so participants may compensate for a part of their data privacy rather than turning off data collection by acknowledging the significance of data collection in research purposes. To mitigate such concerns, conducting further studies in various contexts and with different participant demographics would be beneficial. In terms of contextual filtering, we only offered time and place filtering, neglecting other contextual factors (e.g., data subject, sender, recipients) that may affect privacy decisions [51].

Moreover, we acknowledge a limited generalizability of our findings due to the small sample size and short period. This experiment design was due to the recruiting difficulty and a limited period to complete the experiment. These limitations restricted categorizing user groups based on each system feature level (e.g., dividing participants into four groups with the combination of 1) with/without data exploration feature and 2) with/without contextual filtering feature). To address the issue, increasing the number of participants based on G-power calculation, dividing them according to the presence or absence of each feature, and analyzing the effects would be feasible. Lastly, a three-week user study period raises the question of whether prolonged use of the PriviAware system significantly influences privacy awareness and engagement. Therefore, undertaking a long-term deployment study could also be valuable for future research.

8 CONCLUSION

We introduced PriviAware, a mobile application facilitating flexible data consent in the context of mobile sensing research. We aimed to increase participants' privacy awareness by exploring collected data and pausing data collection based on time and location with contextual filtering. The user study revealed that participants perceived the graphical representations and features of the PriviAware to be intuitive and usable. Regarding the effectiveness of those features, participants responded that the data exploration could raise their awareness of privacy concerns. At the same time, contextual filtering empowered them to proactively control data collection based on privacy-sensitive contexts. The findings offer several design implications of the system for user privacy in the mobile sensing research domain. We expect that our approach can be extended to diverse privacy-by-design solutions fostering user-oriented, responsible privacy data management.

ACKNOWLEDGMENTS

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Korean government (MSIT) (2022R1A2C2011536) and by the KAIST Future Smart Home Research Center grant funded by the Taejae Research Foundation.

REFERENCES

[1] Yuvraj Agarwal and Malcolm Hall. 2013. ProtectMyPrivacy: detecting and mitigating privacy leaks on iOS devices using crowdsourcing. In *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*. 97–110.

[2] 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*. 787–796.

[3] Julio Angulo, Simone Fischer-Hübner, Tobias Pulls, and Erik Wästlund. 2015. Usable transparency with the data track: a tool for visualizing data disclosures. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*. 1803–1808.

[4] Apple. 2018. https://researchkit.org/docs/docs/InformedConsent/InformedConsent.html

[5] 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.

[6] Aaron Bangor, Philip T Kortum, and James T Miller. 2008. An empirical evaluation of the system usability scale. *Intl. Journal of Human–Computer Interaction* 24, 6 (2008), 574–594.

[7] Jakob E Bardram. 2020. The CARP mobile sensing framework–A cross-platform, reactive, programming framework and runtime environment for digital phenotyping. *arXiv preprint arXiv:2006.11904* (2020).

[8] Gillinder Bedi, Facundo Carrillo, Guillermo A Cecchi, Diego Fernández Slezak, Mariano Sigman, Natália B Mota, Sidarta Ribeiro, Daniel C Javitt, Mauro Copelli, and Cheryl M Corcoran. 2015. Automated analysis of free speech predicts psychosis onset in high-risk youths. *npj Schizophrenia* 1, 1 (2015), 1–7.

[9] Marit Bentvelzen, Julia Dominiak, Jasmin Niess, Frederique Henraat, and Paweł W Woźniak. 2023. How Instructional Data Physicalisation Fosters Reflection in Personal Informatics. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–15.

[10] Christoph Bier, Kay Kühne, and Jürgen Beyerer. 2016. PrivacyInsight: the next generation privacy dashboard. In *Privacy Technologies and Policy: 4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016, Proceedings 4*. Springer, 135–152.

[11] Elettra Bietti. 2019. Consent as a free pass: Platform power and the limits of the informational turn. *Pace L. Rev.* 40 (2019), 310.

[12] Debmalya Biswas, Imad Aad, and Gian Paolo Perrucci. 2013. Privacy panel: Usable and quantifiable mobile privacy. In *2013 International Conference on Availability, Reliability and Security*. IEEE, 218–223.

[13] 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.

[14] Virginia Braun and Victoria Clarke. 2012. *Thematic analysis*. American Psychological Association.

[15] Isabelle Budin-Ljøsne, Harriet JA Teare, Jane Kaye, Stephan Beck, Heidi Beate Bentzen, Luciana Caenazzo, Clive Collett, Flavio D'Abramo, Heike Felzmann, Teresa Finlay, et al. 2017. Dynamic consent: a potential solution to some of the challenges of modern biomedical research. *BMC medical ethics* 18, 1 (2017), 1–10.

[16] Saksham Chitkara, Nishad Gothoskar, Suhas Harish, Jason I Hong, and Yuvraj Agarwal. 2017. Does this app really need my location? Context-aware privacy management for smartphones. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 3 (2017), 1–22.

[17] Yves-Alexandre de Montjoye, Jordi Quoidbach, Florent Robic, and Alex Pentland. 2013. Predicting personality using novel mobile phone-based metrics. In *Social Computing, Behavioral-Cultural Modeling and Prediction: 6th International Conference, SBP 2013, Washington, DC, USA, April 2-5, 2013. Proceedings 6*. Springer, 48–55.

[18] 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.

[19] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2021. An informative security and privacy "nutrition" label for internet of things devices. *IEEE Security & Privacy* 20, 2 (2021), 31–39.

[20] Denzil Ferreira, Vassilis Kostakos, and Anind K Dey. 2015. AWARE: mobile context instrumentation framework. *Frontiers in ICT* 2 (2015), 6.

[21] Simone Fischer-Hübner, Julio Angulo, Farzaneh Karegar, and Tobias Pulls. 2016. Transparency, privacy and trust–Technology for tracking and controlling my data disclosures: Does this work?. In *Trust Management X: 10th IFIP WG 11.11 International Conference, IFIPTM 2016, Darmstadt, Germany, July 18-22, 2016, Proceedings 10*. Springer, 3–14.

[22] 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.

[23] Pamela Grimm. 2010. Social desirability bias. *Wiley international encyclopedia of marketing* (2010).

[24] Wentao Guo, Jay Rodolitz, and Eleanor Birrell. 2020. Poli-see: An interactive tool for visualizing privacy policies. In *Proceedings of the 19th Workshop on Privacy in the Electronic Society*. 57–71.

[25] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. 2014. Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 2647–2656.

[26] Yangyang He, Paritosh Bahirat, Bart P Knijnenburg, and Abhilash Menon. 2019. A data-driven approach to designing for privacy in household iot. *ACM Transactions on Interactive Intelligent Systems (TiiS)* 10, 1 (2019), 1–47.

[27] John Hicks, Nithya Ramanathan, Donnie Kim, Mohamad Monibi, Joshua Selsky, Mark Hansen, and Deborah Estrin. 2010. AndWellness: an open mobile system for activity and experience sampling. In *Wireless Health 2010*. 34–43.

[28] Syed Monowar Hossain, Timothy Hnat, Nazir Saleheen, Nusrat Jahan Nasrin, Joseph Noor, Bo-Jhang Ho, Tyson Condie, Mani Srivastava, and Santosh Kumar. 2017. mCerebrum: a mobile sensing software platform for development and validation of digital biomarkers and interventions. In *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*. 1–14.

[29] Bernardo A Huberman, Eytan Adar, and Leslie R Fine. 2005. Valuating privacy. *IEEE security & privacy* 3, 5 (2005), 22–25.

[30] Thomas R Insel. 2017. Digital phenotyping: technology for a new science of behavior. *Jama* 318, 13 (2017), 1215–1216.

[31] 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.

[32] Soowon Kang, Woohyeok Choi, Cheul Young Park, Narae Cha, Auk Kim, Ahsan Habib Khandoker, Leontios Hadjileontiadis, Heepyung Kim, Yong Jeong, and Uichin Lee. 2023. K-EmoPhone: A Mobile and Wearable Dataset with In-Situ Emotion, Stress, and Attention Labels. *Scientific Data* 10, 1 (2023), 351.

[33] 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.

[34] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. 2009. A" nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. 1–12.

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

[36] Jaejeung Kim, Joonyoung Park, Hyunsoo Lee, Minsam Ko, and Uichin Lee. 2019. LocknType: Lockout task intervention for discouraging smartphone app use. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–12.

[37] Evan M Kleiman, Brianna J Turner, Szymon Fedor, Eleanor E Beale, Rosalind W Picard, Jeff C Huffman, and Matthew K Nock. 2018. Digital phenotyping of suicidal thoughts. *Depression and anxiety* 35, 7 (2018), 601–608.

[38] 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.

[39] Interactive Computing Lab. 2024. ABC Logger. https://github.com/Kaist-ICLab/ABCLogger.git.

[40] Hyunsoo Lee, Soowon Kang, and Uichin Lee. 2022. Understanding privacy risks and perceived benefits in open dataset collection for mobile affective computing. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 2 (2022), 1–26.

[41] 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.

[42] Hyunsoo Lee and Uichin Lee. 2022. Toward dynamic consent for privacy-aware pervasive health and well-being: A scoping review and research directions. *IEEE Pervasive Computing* (2022).

[43] Ken Jen Lee, Adrian Davila, Hanlin Cheng, Joslin Goh, Elizabeth Nilsen, and Edith Law. 2023. "We need to do more... I need to do more": Augmenting Digital Media Consumption via Critical Reflection to Increase Compassion and Promote

Prosocial Attitudes and Behaviors. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–20.

[44] Nicola Leonardi, Marco Manca, Fabio Paternò, and Carmen Santoro. 2019. Trigger-action programming for personalising humanoid robot behaviour. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[45] Jong Hyun Lim, Andong Zhan, Evan Goldschmidt, JeongGil Ko, Marcus Chang, and Andreas Terzis. 2012. HealthOS: a platform for pervasive health applications. In *Proceedings of the Second ACM Workshop on Mobile Systems, Applications, and Services for HealthCare*. 1–6.

[46] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM conference on ubiquitous computing*. 501–510.

[47] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Aerin Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. 2016. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Twelfth symposium on usable privacy and security (SOUPS 2016)*. 27–41.

[48] 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.

[49] Ewa Luger and Tom Rodden. 2013. An informed view on consent for UbiComp. In *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*. 529–538.

[50] Ewa Luger and Tom Rodden. 2013. Terms of agreement: Rethinking consent for pervasive computing. *Interacting with Computers* 25, 3 (2013), 229–241.

[51] Nathan Malkin. 2022. Contextual Integrity, Explained: A More Usable Privacy Definition. *IEEE Security & Privacy* 21, 1 (2022), 58–65.

[52] Nicole Martinez-Martin, Thomas R Insel, Paul Dagum, Henry T Greely, and Mildred K Cho. 2018. Data mining for health: staking out the ethical territory of digital phenotyping. *NPJ digital medicine* 1, 1 (2018), 68.

[53] Vivian Genaro Motti and Kelly Caine. 2015. Users' privacy concerns about wearables: impact of form factor, sensors and type of data collected. In *Financial Cryptography and Data Security: FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, January 30, 2015, Revised Selected Papers*. Springer, 231–244.

[54] Jennifer Nicholas, Katie Shilton, Stephen M Schueller, Elizabeth L Gray, Mary J Kwasny, David C Mohr, et al. 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.

[55] Emma Ning, Andrea T Cladek, Mindy K Ross, Sarah Kabir, Amruta Barve, Ellyn Kennelly, Faraz Hussain, Jennifer Duffecy, Scott L Langenecker, Theresa Nguyen, et al. 2023. Smartphone-derived Virtual Keyboard Dynamics Coupled with Accelerometer Data as a Window into Understanding Brain Health: Smartphone Keyboard and Accelerometer as Window into Brain Health. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–15.

[56] 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.

[57] 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.

[58] Van L Parsons. 2014. Stratified sampling. *Wiley StatsRef: Statistics Reference Online* (2014), 1–11.

[59] 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.

[60] Marco V Perez, Kenneth W Mahaffey, Haley Hedlin, John S Rumsfeld, Ariadna Garcia, Todd Ferris, Vidhya Balasubramanian, Andrea M Russo, Amol Rajmane, Lauren Cheung, et al. 2019. Large-scale assessment of a smartwatch to identify atrial fibrillation. *New England Journal of Medicine* 381, 20 (2019), 1909–1917.

[61] Jyoti Prakash, Suprakash Chaudhury, and Kaushik Chatterjee. 2021. Digital phenotyping in psychiatry: When mental health goes binary. *Industrial Psychiatry Journal* 30, 2 (2021), 191.

[62] Andrew Raij, Animikh Ghosh, Santosh Kumar, and Mani Srivastava. 2011. Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 11–20.

[63] General Data Protection Regulation. 2018. General data protection regulation (GDPR). *Intersoft Consulting, Accessed in October* 24, 1 (2018).

[64] 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.

[65] 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.

[66] Sohrab Saeb, Mi Zhang, Christopher J Karr, Stephen M Schueller, Marya E Corden, Konrad P Kording, David C Mohr, et al. 2015. Mobile phone sensor correlates of depressive symptom severity in daily-life behavior: an exploratory study. *Journal of medical Internet research* 17, 7 (2015), e4273.

[67] Hillol Sarker, Matthew Tyburski, Md Mahbubur Rahman, Karen Hovsepian, Moushumi Sharmin, David H Epstein, Kenzie L Preston, C Debra Furr-Holden, Adam Milam, Inbal Nahum-Shani, et al. 2016. Finding significant stress episodes in a discontinuous time series of rapidly varying mobile sensor data. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 4489–4501.

[68] Lydia Sequeira, Marco Battaglia, Steve Perrotta, Kathleen Merikangas, and John Strauss. 2019. Digital Phenotyping With Mobile and Wearable Devices: Advanced Symptom Measurement in Child and Adolescent Depression. *Journal of the American Academy of Child and Adolescent Psychiatry* 58, 9 (2019), 841–845.

[69] 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.

[70] Fuming Shih, Ilaria Liccardi, and Daniel Weitzner. 2015. Privacy tipping points in smartphones privacy preferences. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 807–816.

[71] Ida Sim. 2019. Mobile devices and health. *New England Journal of Medicine* 381, 10 (2019), 956–968.

[72] Hongsuda Tangmunarunkit, Cheng-Kang Hsieh, Brent Longstaff, S Nolen, John Jenkins, Cameron Ketcham, Joshua Selsky, Faisal Alquaddoomi, Dony George, Jinha Kang, et al. 2015. Ohmage: A general and extensible end-to-end participatory sensing platform. *ACM Transactions on Intelligent Systems and Technology (TIST)* 6, 3 (2015), 1–21.

[73] Jing Xian Teo, Sonia Davila, Chengxi Yang, An An Hii, Chee Jian Pua, Jonathan Yap, Swee Yaw Tan, Anders Sahlén, Calvin Woon-Loong Chin, Bin Tean Teh, et al. 2019. Digital phenotyping by consumer wearables identifies sleep-associated markers of cardiovascular disease risk and biological aging. *Communications Biology* 2, 1 (2019), 361.

[74] John Torous, Mathew V Kiang, Jeanette Lorme, Jukka-Pekka Onnela, et al. 2016. New tools for new research in psychiatry: a scalable and customizable platform to empower data driven smartphone research. *JMIR mental health* 3, 2 (2016), e5165.

[75] John Torous, Mark E Larsen, Colin Depp, Theodore D Cosco, Ian Barnett, Matthew K Nock, and Joe Firth. 2018. Smartphones, sensors, and machine learning to advance real-time prediction and interventions for suicide prevention: a review of current progress and next steps. *Current psychiatry reports* 20 (2018), 1–6.

[76] John Torous and Adam C Powell. 2015. Current research and trends in the use of smartphone applications for mood disorders. *Internet Interventions* 2, 2 (2015), 169–173.

[77] John Torous, Patrick Staples, and Jukka-Pekka Onnela. 2015. Realizing the potential of mobile mental health: new methods for new data in psychiatry. *Current psychiatry reports* 17 (2015), 1–7.

[78] Lynn Tsai, Primal Wijesekera, Joel Reardon, Irwin Reyes, Serge Egelman, David Wagner, Nathan Good, and Jung-Wei Chen. 2017. Turtle guard: Helping android users apply contextual privacy preferences. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 145–162.

[79] Elena Vildjiounaite, Johanna Kallio, Vesa Kyllönen, Mikko Nieminen, Ilmari Määttänen, Mikko Lindholm, Jani Mäntyjärvi, and Georgy Gimel'farb. 2018. Unobtrusive stress detection on the basis of smartphone usage data. *Personal and Ubiquitous Computing* 22 (2018), 671–688.

[80] 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.

[81] 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.

[82] Xuancong Wang, Nikola Vouk, Creighton Heaukulani, Thisum Buddhika, Wijaya Martanto, Jimmy Lee, and Robert JT Morris. 2021. HOPES: an integrative digital phenotyping platform for data collection, monitoring, and machine learning. *Journal of medical Internet research* 23, 3 (2021), e23984.

[83] Mark Weiser. 1999. The computer for the 21st century. *ACM SIGMOBILE mobile computing and communications review* 3, 3 (1999), 3–11.

[84] Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov. 2017. The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1077–1093.

[85] Daricia Wilkinson, Paritosh Bahirat, Moses Namara, Jing Lyu, Arwa Alsubhi, Jessica Qiu, Pamela Wisniewski, and Bart P Knijnenburg. 2020. Privacy at a glance: the user-centric design of glanceable data exposure visualizations. (2020).

[86] Jong-bum Woo and Youn-kyung Lim. 2020. Routinoscope: Collaborative routine reflection for routine-driven do-it-yourself smart homes. *International Journal of Design* 14, 3 (2020), 19.

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

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

[89] 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.

[90] Ka-Ping Yee. 2002. User interaction design for secure systems. In *International Conference on Information and Communications Security*. Springer, 278–290.

[91] Valerie Zhao, Lefan Zhang, Bo Wang, Michael L Littman, Shan Lu, and Blase Ur. 2021. Understanding trigger-action programs through novel visualizations of program differences. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–17.