Original Paper

Breaking the Data Value-Privacy Paradox in Mobile Mental Health Systems Through User-Centered Privacy Protection: A Web-Based Survey Study

Dongsong Zhang, PhD; Jaewan Lim, MSc; Lina Zhou, PhD; Alicia A Dahl, PhD

The University of North Carolina at Charlotte, Charlotte, NC, United States

Corresponding Author:
Dongsong Zhang, PhD
The University of North Carolina at Charlotte
9201 University City Blvd
Charlotte, NC, 28223-0001
United States
Phone: 1 7046871893
Email: dzhang15@uncc.edu

Abstract

Background: Mobile mental health systems (MMHS) have been increasingly developed and deployed in support of monitoring, management, and intervention with regard to patients with mental disorders. However, many of these systems rely on patient data collected by smartphones or other wearable devices to infer patients' mental status, which raises privacy concerns. Such a value-privacy paradox poses significant challenges to patients' adoption and use of MMHS; yet, there has been limited understanding of it.

Objective: To address the significant literature gap, this research aims to investigate both the antecedents of patients' privacy concerns and the effects of privacy concerns on their continuous usage intention with regard to MMHS.

Methods: Using a web-based survey, this research collected data from 170 participants with MMHS experience recruited from online mental health communities and a university community. The data analyses used both repeated analysis of variance and partial least squares regression.

Results: The results showed that data type (P=.003), data stage (P<.001), privacy victimization experience (P=.01), and privacy awareness (P=.08) have positive effects on privacy concerns. Specifically, users report higher privacy concerns for social interaction data (P=.007) and self-reported data (P=.001) than for biometrics data; privacy concerns are higher for data transmission (P=.01) and data sharing (P<.001) than for data collection. Our results also reveal that privacy concerns have an effect on attitude toward privacy protection (P=.001), which in turn affects continuous usage intention with regard to MMHS.

Conclusions: This study contributes to the literature by deepening our understanding of the data value-privacy paradox in MMHS research. The findings offer practical guidelines for breaking the paradox through the design of user-centered and privacy-preserving MMHS.

(JMIR Ment Health 2021;8(12):e31633) doi: 10.2196/31633

KEYWORDS

mobile apps; mental health; privacy concerns; privacy protection; mobile phone

Introduction

Patient Data Privacy

Mental health, including emotional, psychological, and social well-being, affects how people think, feel, and act. According to the National Alliance on Mental Illness, in the United States, 1 in 5 adults experience a mental illness; depression, a type of mental disorder, is the leading cause of disability worldwide; and 90% of the people who commit suicide have mental illness. Recent trends in the health care industry have been driving significant changes in the health information technology landscape, including the movement toward developing effective technologies that enable continuous data collection from patients through mobile and wearable devices [1]. Examples of these trends include the shift of health care systems toward more efficient yet less expensive methods of patient care; strong economic incentives to pursue continuous patient monitoring

outside clinical settings and innovative technologies to prevent patients from falling ill; increasing adoption of mobile and wearable devices such as smartphones and biological sensors by patients, caregivers, and health care service providers for health and wellness apps; and technology advances that increase the utility of mobile devices [1].

Rapid advances in wireless communication, low-power sensing technologies, and pervasive mobile and wearable devices (eg, smartphones, smart watches, and Fitbit) propel research on, and practice of, mobile health (mHealth), including mobile mental health (MMH). According to the Pew Research Center [2], 81% of American adults have a smartphone. More than 60% of people have downloaded an mHealth app, with more than 300,000 mHealth apps available. The main features of mHealth apps include symptom checkers, health care professional finders, management of clinical records, medical education and training, patient monitoring, patient self-management, and prescription filling and compliance [3].

MMH systems (MMHS) collect unprecedented amounts and varieties of data through sensors, smartphones, or other wearable devices in support of continuous monitoring, self-management, and intervention with regard to patients with mental illness or patients' well-being. These data enable researchers to quantify complex temporal dynamics of important physical (eg, body movement), biological (eg, skin temperature and heart rate), behavioral (eg, phone use behavior and keystrokes), psychological (eg, emotion), social (eg, social interactions with others such as phone calls and SMS text messaging), and environmental factors (eg, location and lighting) that may be affected by, or be indicative of, mental illness [4-6]. Thus, MMH technology has great potential to yield new insights, increase health care agility and quality, extend ubiquitous access to health care resources and services, reduce hospital admissions and cost, and improve personal wellness and public mental health.

These benefits, however, can only be achieved if the health-related data continuously collected from individuals by MMHS are appropriately protected for user privacy. The general notion of privacy is perceived as a human right, a commodity, and control [7]. This research focuses on patient data privacy during collection, transmission, storage, and sharing of personal data. Unlike data security, which refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure [8], health information privacy is an individual's right to control the acquisition, use, or disclosure of their identifiable health-related data, including when, how, and to what extent the data can be communicated to others [9]. Vulnerabilities regarding privacy may result in breaching the confidentiality of patient data [10], leading to financial losses, discrimination, stress, dissatisfaction, or even delays in seeking timely treatment because of perceived privacy risks. Individuals with high privacy concerns often perceive a new information system to be risky, eventually developing concerns about it [10].

Despite its potential, mHealth research and practice has progressed much more slowly than app developments in the industry because privacy issues remain an ongoing concern because of the sensitive, personal, and streaming nature of data collected from individual patients by sensors or other wearable devices [11]. Our literature review reveals that approximately half of the surveyed studies on MMHS [12-14] did not consider data privacy issues at all. Prior research also suggests that users lack understanding of privacy issues associated with mHealth technologies [9]. Although some studies adopted certain user privacy protection methods, most of them deployed a single method (eg, data encryption [15-17] and extracting and storing features of data instead of original content [18,19]). A number of studies have shown that users sometimes sacrifice their privacy in exchange for benefits and personalized services [20,21]. Different types of information may have different levels of overall "privateness [22]." There is a severe lack of studies and comprehensive understanding of users' privacy concerns with different types of personal data collected and used by MMHS and how to address them to increase users' adoption of, and engagement with, these systems [23].

According to the privacy calculus theory [24], an individual's intention to disclose personal information is based on their perceived risk and anticipated benefits. On the one hand, it is theoretically desirable for MMHS to collect as much (and detailed) relevant personal data as possible from individuals that are indicators of mental health so that the systems can predict the individuals' mental status more accurately and make more informed intervention decisions. On the other hand, it remains uncertain how sensitive, in terms of privacy, users are to different types of personal data being collected, which data processing stages may cause them to have privacy concerns, and to what extent privacy concerns may influence their willingness to use MMHS. To help address the data value-privacy paradox, this study aims to answer the following research questions:

- Research question 1: How do users' privacy concerns vary with different types of personal data collected by MMHS?
- Research question 2: Do users' privacy concerns vary with different data processing stages that MMHS involve? If so, how?
- Research question 3: How do privacy concerns affect users' intention of using MMHS?

To answer these research questions, we conducted a web-based survey with adults who have self-reported mental health issues and used MMHS before. On the basis of the findings of our survey, we propose a set of guidelines for the design of user-centric and privacy-protecting MMHS. This study contributes to MMHS research by deepening our understanding of users' privacy concerns and potential mitigation solutions. In addition, it offers practical implications for improving the well-being of patients with mental illness by cultivating their adoption of, and engagement with, MMHS.

Background and Related Work

Conceptualization of Privacy

Generally, privacy can be categorized into physical privacy and information privacy (also commonly referred to as data privacy). Historically, the concept of physical privacy was defined as "the right to be left alone [25]." Information privacy is concerned not only with individuals' personal information such

as name, home address, and birth date, but also their relationship status, photographs, political and religious views, shopping habits, driving history, and medical records [26]. It also involves an individual's ability to control information about themselves [27]. Information privacy is also referred to as controlling whether and how personal data can be collected, stored, processed, and disseminated [28]. As technologies evolve, privacy has been increasingly threatened as a result of the rapid growth of portable handheld devices, sensors, and wireless network technology. Accordingly, the conceptualizations of privacy have shifted toward elaborating the complexity of privacy issues in various areas involving the legal, social-psychological, economic, or political concerns that technologies present.

Smith et al [7] proposed a macro model called "Antecedents→Privacy Concerns→Outcomes" that demonstrated the relationships between privacy concerns and their antecedents and outcomes. The model shows that individuals' experiences with getting exposed to, or victimized by, personal information abuses; privacy awareness; personality (eg, introversion vs extroversion); demographics; and cross-cultural differences are antecedents of privacy concerns. Privacy concerns in turn affect behavioral reactions (eg, willingness to disclose information), trust, regulation, and privacy calculus (ie, trade-off between privacy risks and benefits).

Plachkinova et al [29] developed a taxonomy based on security challenges in an mHealth care environment defined by Stavrou and Pitsillides [30] and the threat taxonomy for mHealth privacy proposed by Kotz [31]. Plachkinova et al [29] identified a few common threats to privacy, including (1) identity threats: misuse of patient identity information; (2) access threats: unauthorized access to protected health information (PHI) or personal health records; and (3) disclosure threats: unauthorized disclosure of patient identity information or PHI. However, the authors' taxonomy neither differentiates data types nor considers user privacy protection.

Privacy Regulations

Privacy regulations have been established to help determine effective ways to develop, manage, monitor, and enforce patient-centric, organizational, and government policies and regulations associated with data collection and use within mHealth systems [32]. For example, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 provides data privacy and security guidelines for safeguarding medical information and sets constraints and conditions for the use and disclosure of patient information (Textbox 1). HIPAA's privacy rule only applies to mHealth apps that involve both a covered entity (eg, health care providers) and PHI. PHI usually includes demographic information, medical history, diagnostic test results, insurance information, and other data gathered by a health care professional that identify an individual and are used for medical treatment. HIPAA does not cover individual users who upload or directly enter their information into mHealth apps [33]. In addition, researchers must abide by the federal policy for the protection of human subjects, also known as the Common Rule, to protect individuals participating in research activities. The Common Rule specifies detailed policies and guidelines about informed consent, adverse events, handling of biological data, and vulnerable populations, among other issues [34].

Textbox 1. The Health Insurance Portability and Accountability Act privacy and security requirements (adapted from Ray and Biswas [35]).

Privacy and security requirements

- Patients' understanding
- Patients have the right to understand how their health information will be used and stored.
- Patient control
- Patients can control the access to their health information and are given permission to decide who can access their health data.
- Confidentiality
- Health data of patients must be kept undisclosed from any party that has no right to access the data.
- There should be software safeguards such as encryption to protect health data confidentiality during storage and transmission.
- Data integrity
- Patients' eHealth information should be protected from omissions, tampering, and unauthorized destruction.
- The health data shared with an entity must be the true representation of the intended information without having any form of alteration.
- Consent exception
- In life-saving purposes and emergency situations, access to the protected health information without the patient's authorization is allowed.

The most recent US privacy regulation is the California Consumer Privacy Act, which provides California residents transparency and protection of personal data, including the right to know where their data are collected and to whom they are sold, as well as the right to disclose. In 2019, Xcertia [36] published the following industry guidelines for safe and effective mHealth apps:

- Guideline P1: Notice of Use and Disclosure. The Privacy Notice describes how an organization collects, uses, and retains user data.

- Guideline P2: Retention. If data are collected, the user shall be informed about how long the data will be retained.
- Guideline P3: Access Mechanisms. An app user should be informed if the app accesses local resources or resources from, or for, social networking platforms, provided with an explanation by any appropriate means (eg, the About section) as to how and why such resources are used, and opt-in consent should be obtained to access such resources.
- Guideline P4: HIPAA Entity or Business Associate. If a mobile app collects, stores, or transmits information that constitutes PHI (as defined by HIPAA), it does so in full compliance with HIPAA and all applicable state and international regulations.
- Guideline P5: Children's Online Privacy Protection Act. An app should have measures in place to protect children in accordance with applicable laws and regulations if the website is directed at children.
- Guideline P6: General Data Protection Regulation. An app should have measures in place to comply with applicable laws and regulations related to the European Union General Data Protection Regulation.

Personal Data Collected by Existing MMH Studies

To understand what personal data have been collected by existing MMH studies and whether these studies have deployed any privacy protection method, we first conducted a literature review. We formulated search queries as various combinations of terms from 3 groups, including technology terms such as "mobile," "wearable devices," "sensor," "IoT," and "mobile app;" mental health terms such as "mental health," "depression," "schizophrenia," and "stress management" used by Bardram and Matic [37] and the US Department of Health and Human Services; and privacy-related search terms such as "privacy," "privacy protection," "personal," and "private information." We searched for relevant articles in the following databases: PubMed, IEEE Xplore, National Institute of Mental Health Data Archive, ScienceDirect, Taylor & Francis Online, and PubPsych, as well as Google Scholar. We applied 3 inclusion criteria in paper selection: (1) published in English in or after 2014 to reflect the state of the art, (2) focused on MMHS in support of users with an existing mental disorder, and (3) collected personal data from users.

We found and reviewed 32 papers that met the aforementioned inclusion criteria. These studies [4-6,12-19,38-58] are summarized in Multimedia Appendix 1 along the following dimensions: the target mental diseases that the MMHS were proposed to support, types of personal data collected by the apps, and privacy protection methods deployed in these studies, if any. These studies collected a wide variety of personal data from patients, driven by the target mental diseases. The most commonly used personal data are as follows:

- Physical activities such as gait, finger tapping, activity time, and distance traveled
- Sleep data such as sleeping time and waking time
- Physiological data (biomarkers) such as oxygen saturation, heart rate, temperature, blood pressure, electrocardiogram, and peak expiratory flow rate
- Location and GPS data
- Social activity (ie, social interaction) data
- Phone use such as number and length of phone calls, number of incoming and outgoing SMS text messages, and the number of times screen is on
- Voice

Privacy Protection Adopted by Existing MMHS Studies

Not surprisingly, of the 32 surveyed studies, 11 (34%) did not mention any user privacy protection, as shown in Multimedia Appendix 1. This finding is in line with the findings of previous studies. For example, Nurgalieva et al [59] found that only a third of their reviewed mHealth papers considered privacy and security together. A recent survey study revealed that most (68%) of the reviewed MMHS were not sufficiently transparent regarding privacy protection information, whereas more than half had no privacy policy at all [60]. Furthermore, the study found that even in the case of mobile apps that had a privacy policy, researchers collected data without informing users about how the data would be used [60].

We categorized the user privacy protection mechanisms implemented in our surveyed studies into the following types: data anonymization; encryption (when transferring data from local mobile devices to remote data storage [eg, cloud storage]); access control; archiving only features extracted from the original data, instead of the original data; and allowing certain collected data to be wiped out remotely by users. Among them, data anonymization and encryption were the most common mechanisms used. A shared key is needed in the process of encryption and decryption, and, according to federal HIPAA and Health Information Technology for Economic and Clinical Health Act regulations, the key length must be 128 bits. The National Institute of Standards and Technology recommends using Suite-B, a set of algorithms that exchange decryption keys and digital signatures to authenticate data [9].

Despite the use of data anonymization and encryption having become common, there are still risks of data breach and disclosure, given that original data are stored physically. In comparison, archiving only selective features extracted from collected user data and allowing users to delete any collected data may help alleviate the risk of disclosure of, or unauthorized access to, personally sensitive data. For example, real-time audio processing can be used to extract relevant health inferences (ie, features) while discarding sensitive content. Of note, this option of privacy protection does not come without a cost—there is always a trade-off between user privacy and data utility: the fewer data points that MMHS collect, the higher the degree of user privacy protection but the more inferior the services they provide. For example, disabling collection of data about users' physical activities or social interactions will help alleviate users' privacy concerns, but it may also negatively affect the benefits of MMHS (eg, depression detection) because the systems may not infer users' mental status accurately because of the removal of such data. By analogy, in e-commerce, consumers may sacrifice their privacy to some extent by allowing cookies to capture their behavior on an online retailer's website to receive personalized services (eg, personalized product recommendations) [61]. Therefore, understanding user perceptions of different types of personal data with regard to

privacy and developing and deploying effective privacy protection methods have the potential to break the value-privacy paradox, which will ultimately influence user adoptions and continuous use of MMHS.

The Research Model and Hypotheses

As summarized in the previous section, existing MMHS have collected various types of personal data. We investigate privacy concerns mainly from the 2 dimensions in this research: data type and data stage.

Researchers have found that the same individuals may have different levels of privacy concerns for different types of personal information [62]. For instance, online shoppers tend to be more likely to withhold information such as purchase history, social security number, hobbies, and favorite websites than name, gender, and education information [63]. Geographic location, mailing address, and information about friends and profession were common data types that a sample of 1000 French online users reported unwilling to disclose [64]. From a social media perspective, interaction with others through social networks usually leads to generating and sharing personal information actively [65]. Jin [66] suggests that although Twitter users often share personal information about their daily lives and entertainment choices, they would hardly reveal their own mental or physical health information. Thus, we propose the first hypothesis as follows:

Hypothesis 1. Data type has an effect on user privacy concerns with MMHS.

Data processing stages can be another critical dimension of privacy in MMHS. Data processing starts with data *collection*. Because of limited storage space as well as limited processing power of a mobile or wearable device (eg, smartphone), the data collected by MMHS are typically transferred to a remote server or to the cloud for processing and storage, which will finally lead to data sharing. Xu (2019) characterizes the combination of health informatics and cloud computing as Health Informatics as a Service [67]. Hindy et al (2020) emphasize the threats of personal information leakage at a data transmission level because mobile apps are increasingly dependent on wireless networks, which raises privacy concerns when transmitting data wirelessly [68]. Zeissig et al [69] and Kotz [33] suggest that privacy concerns vary with an app's functionality and the entities that process data. Given that the data at different stages can be exposed to different levels of privacy risks and data transmission and data sharing are particularly vulnerable to intrusion with regard to data privacy, we propose the second hypothesis as follows:

Hypothesis 2. Data stage has an effect on user privacy concerns with MMHS.

Hypothesis 2.1. Privacy concerns for the (i) data transmission and (ii) data sharing stages are higher than those for the data collection stage.

Hypothesis 2.2. Privacy concerns for the (i) data transmission and (ii) data sharing stages are higher than those for the data storage stage.

Privacy awareness refers to the extent to which individuals are well informed about privacy practices and privacy breach incidents around themselves [70]. A number of studies have found that privacy awareness is positively associated with privacy concerns in the context of computer use [71], peer relationships on social media [72], older generation's online privacy perception [69], personal cloud storage apps [73], news content ownership on social media [74], and so on.

Privacy victimization experience has been shown to influence privacy concerns in previous studies [70-72,75,76]. Privacy calculus theory [24] posits that individuals tend to weigh potential benefits and risks of data disclosure decisions. They will disclose personal information when the perceived benefits exceed the potential cost. If they have been previously victimized by privacy disclosure, they may perceive the cost of data disclosure to be higher than the benefit and be hesitant to take a risk. Therefore, previous experience of having been a victim of privacy intrusion could result in MMHS users assessing risks and foreseeing future consequences of privacy intrusion better. For example, Chen et al [77] suggest that online scam victims have higher perceived threat than nonvictims. Most victims of personal information breaches feel fearful, angry, and depressed after being victimized, leading to greater privacy concerns than before [78]. Bansal et al [75] suggest that privacy victimization experience would significantly increase when disclosing private information online. This positive relationship between privacy victimization experience and privacy concerns has also been demonstrated in e-commerce [76], internet use for general purposes [79], social network platforms [80,81], allowing permission requests for data acquisition by mobile apps [82], and Android app downloads [83]. Thus, we predict that people with a higher level of privacy awareness and privacy victimization experience would be more sensitive and concerned about privacy when using MMHS. Therefore, we propose the following 2 hypotheses:

Hypothesis 3. Privacy awareness is positively associated with privacy concerns about MMHS.

Hypothesis 4. Privacy victimization experience is positively associated with privacy concerns about MMHS.

An agreeable attitude toward privacy protection has been suggested as one of the major outcomes of privacy concerns [84,85]. For example, when an individual has a significant privacy concern, they would likely change their online account passwords more frequently than those with lower privacy concerns [77]. Deleting cookies, using ad blockers, and choosing a browser mode that keeps browsing history hidden are typical privacy protection methods used when browsing the web [86]. Similarly, users of social media [87,88] and e-commerce services [89] also seem to look for personal information protection after recognizing privacy risks.

Privacy literacy is another predictor of an agreeable attitude toward privacy protection. Self-control theory [77] posits that one's ability to regulate emotions, behaviors, and desires is determined by one's general intelligence and prior training. People who have high self-control derived from intelligence and sufficient training are likely to pursue a good way of solving a problem [90]. Accordingly, it is reasonable to predict that the

level of a user's privacy literacy, such as HIPAA knowledge level, may influence their privacy concerns about MMHS. Therefore, we hypothesize a positive relationship between HIPAA knowledge level and an agreeable attitude toward privacy protection as follows:

Hypothesis 5. Privacy concerns are positively associated with an agreeable attitude toward privacy protection in MMHS.

Hypothesis 6. HIPAA knowledge level is positively associated with an agreeable attitude toward privacy protection in MMHS.

Privacy protection methods can be viewed as solutions to coping with users' privacy concerns. The Protection Motivation Theory explains how fear may change one's attitude and behavior [91,92]. If an event incurs fear, one may try to reduce unstable emotional state and seek alternative ways in which one can find adaptive coping responses. In the context of MMHS, fear may arise from privacy concerns triggered by threats to personal information. Several studies have explored the relationship between the attitude toward privacy protection and intention to use mHealth systems [37,38]. Attitudes toward privacy protection involve a positive perception of usefulness and optimistic expectation of specific methods. It has been found that users' perceived usefulness of health Internet of Things systems has a significant impact on their intention to use the systems [93]. For example, consumers tend to have a stronger willingness to use health recommendation systems when they feel that the latter are useful for fulfilling their health goals [94]. Employees' optimistic attitudes toward their mobile devices have also been found to have a positive impact on users' intention to use a mobile device in the workplace [95]. Therefore, we propose the following hypothesis:

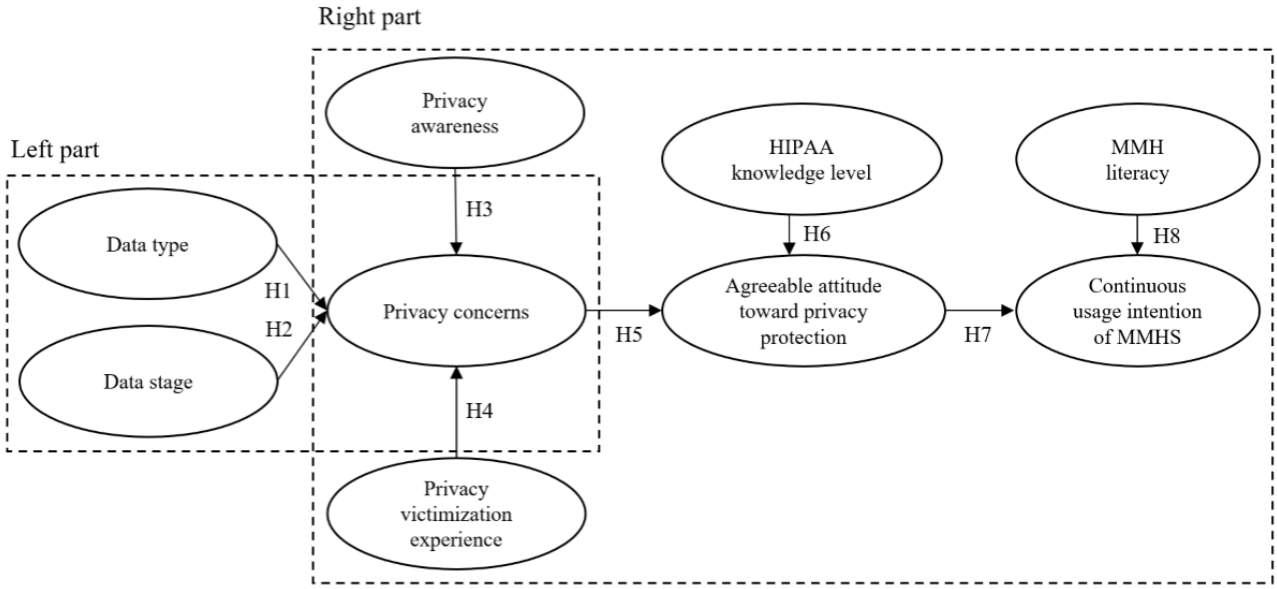
Hypothesis 7. An agreeable attitude toward privacy protection is positively associated with the continuous usage intention of MMHS.

MMH literacy [96,97] plays an important role in the context of health care systems. Zhang and Yan [98] reported that eHealth literacy affected users' continuous intention to use mHealth apps. Drawing on the Elaboration Likelihood Model [99], they suggested that eHealth literacy would foster satisfactory emotions for apps, which in turn motivated continuous intention to use them. Britt et al [100] demonstrated that a higher literacy level measured by the eHealth Literacy Scale led to a greater intention to use online health resources. In the same vein, Kim et al [101] found that mental health literacy would promote help-seeking behavior of college students. Therefore, we expect that patients with higher levels of MMH literacy may understand the potential benefits of MMHS better and accordingly are more likely to use them. Hence, we propose the following hypothesis:

Hypothesis 8. MMH literacy is positively associated with the continuous usage intention of MMHS.

Our research model is shown in Figure 1.

Figure 1. The research model (H: hypothesis; HIPAA: Health Insurance Portability and Accountability Act; MMH: mobile mental health; MMHS: mobile mental health systems).



Methods

To test the hypotheses, we conducted a web-based survey to collect data after receiving approval from the institutional review board of our institution.

Survey Instruments and Procedure

Given that this study is targeted at a specific population, we deployed a prescreening questionnaire to determine participants' eligibility for the study. The eligibility criteria were as follows: participants who (1) were aged ≥18 years, (2) had mental health issues in the past 12 months, and (3) had used any MMHS in the past 12 months. Only qualified participants could proceed with the formal survey.

The formal survey questionnaire (Multimedia Appendix 2) consisted of 3 parts: part 1 collected information about participants' basic demographics, mHealth literacy, and knowledge about HIPAA; part 2 consisted of questions about participants' use of MMHS and their prior experience with privacy protection methods; and part 3 asked questions about

privacy concerns with regard to different data stages and data types. As discussed in the previous section, we considered the following 4 data stages: collection, transmission, storage, and sharing. In addition, we drew on the literature and identified the following 8 types of personal data: physiological signals, voice features, physical activities, facial expression, GPS location, social activities, device use, and self-reported data (Multimedia Appendix 1). Our design of the questionnaire for the agreeable attitude toward privacy protection, which was also based on the findings of our literature review (Multimedia Appendix 1), consisted of 11 items corresponding to the following privacy protection methods: (1) displaying privacy policy, (2) obtaining user consent, (3) disabling collection of personally identifiable data, (4) user control, (5) encryption, (6) secure data transmission, (7) restriction of data storage access, (8) location protection, (9) feature extraction from audio data, (10) feature extraction from text data, and (11) data retraction. All the survey questions were rated on a 7-point Likert scale, ranging from strongly disagree (score=1) to strongly agree (score=7), with a score of 4 being neutral. The details of the relevant questionnaire items are presented in Multimedia Appendix 3 [102-104] and Multimedia Appendix 4 [72,75,87,88,93,94,96,100,105,106].

To ensure data quality, we incorporated 3 attention-check questions into the survey, such as "Please skip this question and do not select anything." We excluded from data analysis the data collected from the participants who failed to follow the instruction while responding to these questions.

Participants

We recruited participants from multiple venues such as online mental health communities (eg, the depression community on Reddit [n=159], the anxiety community on Reddit [n=134], and the mental health group on Facebook [n=55]).

Among the 348 respondents who successfully passed the prescreening test questions, 134 (38.5%) failed the attention-check questions and another 44 (12.6%) completed the survey in an amount of time that was more than 3 SDs from the average time used by the participants of a pilot study. At the end, we obtained 48.9% (170/348) of valid responses. The demographic information of these respondents is presented in Table 1. Each participant was offered a US $5 Amazon gift card for completing the survey.

Table 1. Demographic statistics of the survey respondents (N=170).

Demographic characteristics	Participants, n (%)
Age (years)	
18-25	47 (27.6)
26-30	71 (41.7)
31-35	42 (24.7)
36-40	7 (4.1)
41-45	3 (1.8)
Gender	
Female	61 (35.9)
Male	109 (64.1)
Education	
High school graduate	3 (1.8)
Some college	89 (52.4)
College graduate	55 (32.4)
Postgraduate degree	13 (7.6)
Some postgraduate work	10 (5.9)
Marital status	
Married	82 (48.2)
Single	79 (46.5)
Divorced	9 (5.3)

Data Analysis

We tested the left part of the model using a 2-way repeated analysis of variance and deployed partial least squares (PLS) regression for the right part of the model (Figure 1) using SmartPLS software [107]. It is commonly recognized that correlations among independent variables might increase the variance and lower the power of regression analysis [108,109]. In view of the large number of data types considered in our research design, we first performed a principal component analysis through varimax rotation with Kaiser normalization [110] to identify the principal components based on the

eigenvalues and corresponding eigenvectors of the covariance matrix. Next, based on the results, we selected 4 principal components that explained more than 82% of the variance of the original data types. Specifically, physiological signals, voice features, physical activities, and facial expressions were grouped together and labeled as *biometric factors*, whereas GPS location and social activities were grouped together and labeled as *social interactions*. The remaining original data types—*self-reported data* and *device use*—were left unchanged. These 4 data types were used in subsequent data analyses.

To support PLS regression analysis, we first examined the convergent validity and discriminant validity of the research constructs, which are critical building blocks of model evaluation. We tested the convergent validity with Cronbach α [111], composite reliability with rho_A [112], and discriminant validity with average variable extracted. Following the suggestion of Henseler et al [113], we further assessed the discriminant validity by applying the Heterotrait-Monotrait ratio of correlations. Correlations among the constructs are presented in Multimedia Appendix 5.

Results

Descriptive Statistics and Construct Validations

The test results of convergent and discriminant validity are reported in Table 2. They show that the internal consistency of all reflective constructs (ie, continuous usage intention, MMH literacy, privacy awareness, privacy victimization experience, and HIPAA knowledge level) was acceptable, with Cronbach α>.75. In addition, both their composite reliability and rho_A values exceed the cutoff threshold (0.70) [112]. The average variable extracted results show that all values were >0.60, the acceptable level [114]. The discriminant validity among the reflective constructs is further established based on the Heterotrait-Monotrait ratio of correlations (<0.90; Multimedia Appendix 6). The detailed factor loadings of the constructs and indicators are reported in Multimedia Appendix 7.

Table 2. Construct reliability and validity (reflective constructs only).

Constructs	Cronbach α	rho_A	Composite reliability	Average variable extracted
Continuous usage intention	.759	0.764	0.862	0.675
MMH[a] literacy	.892	0.899	0.915	0.607
Privacy awareness	.829	0.834	0.886	0.660
Privacy victimization experience	.842	0.872	0.892	0.630
HIPAA[b] knowledge level	1.000	1.000	1.000	1.000

[a]MMH: mobile mental health.

[b]HIPAA: Health Insurance Portability and Accountability Act.

The top 3 most common mental health issues of the participants based on their self-reports were depression (33), dysthymia (30), and anxiety (24). According to Wasil et al [115], there are approximately 325,000 mobile apps for health and wellness in the market (ie, Google Play and Apple App Store). Calm [116], Talkspace [117], PTSD (posttraumatic stress disorder) Coach [118], and Optimism [119] are the most commonly used MMHS among our survey respondents. Calm helps users practice meditation and sleep by providing mindfulness music and bedtime stories. It mainly collects data of users' daily app use and time spent on meditating. Talkspace is designed to match a licensed mental health therapist with a user conveniently and affordably in comparison with in-person therapy. Talkspace allows users to submit text, image, and video data regarding their mental status when consulting therapists. PTSD Coach supports those who have PTSD. It gathers users' self-assessment data of PTSD symptoms and daily app use data. Optimism is a mobile app used to track a user's mood level on a daily basis as reported by users with mood disorder.

On the basis of the results of the principal component analysis, we identified 4 main personal data types with respect to privacy concerns, including the degree of privacy concerns arising from *biometric factors*, *social interactions*, *device use*, and *self-reported data*. The descriptive statistics of privacy concerns and other research constructs are reported in Tables 3 and 4, respectively. For all the variables in Tables 3 and 4, their median, maximum, and minimum values are 5, 7, and 1, respectively.

Table 3. Descriptive statistics of privacy concerns.

Research constructs and variables	Values, mean (SD)
Data type	
Biometric factors	4.66 (1.89)
Social interaction	4.89 (1.71)
Device use	4.70 (1.76)
Self-reported data	4.92 (1.84)
Data stage	
Collect	4.61 (1.83)
Store	4.67 (1.83)
Transmit	4.80 (1.82)
Share	4.92 (1.82)

Table 4. Descriptive statistics of other constructs.

Research constructs and variables	Values, mean (SD)
Privacy awareness	4.77 (1.75)
Privacy concerns (composite)	4.75 (1.83)
Privacy victimization experience	4.44 (1.96)
Agreeable attitude toward privacy protection (composite)	5.09 (1.57)
MMH[a] literacy	4.84 (1.69)
HIPAA[b] knowledge level	4.14 (1.92)
Continuous usage intention	5.04 (1.54)

[a]MMH: mobile mental health.

[b]HIPAA: Health Insurance Portability and Accountability Act.

Effects of Data Type and Data Stage

We conducted a 2-way repeated analysis of variance by using privacy concerns as the dependent variable and data type and data stage as the independent variables. The results are reported in Table 5. The analyses yielded significant main effects of data type (P=.003) and data stage (P<.001), as well as their significant interaction effect (P=.008) on privacy concerns.

Table 5. Analysis of variance results for the effects of data type and data stage on privacy concerns.

Sources	F test (df)	Mean squared errors	P value
Data type	4.73 (3,507)	11.78	.003
Data stage	9.35 (3,507)	15.46	<.001
Data type×data stage	2.47 (9,1521)	2.25	.008

The results of post hoc multiple comparisons of the effects of data type and data stage are reported in Tables 6 and 7, respectively. The analysis results of data type show that social interaction data (P=.007) and self-reported data (P=.001) raise greater privacy concerns than biometrics data. In addition, social interaction data cause higher privacy concerns than device use data (P=.045), whereas device use data provoke privacy concerns more than self-reported data (P=.02).

Table 6. Results of comparison of privacy concerns across data types.

Data type (I) and data type (J)	Mean difference (I–J)	*P* value	SE
Biometrics factors			
Social interaction	–0.232	.007	0.084
Device use	–0.044	.53	0.070
Self-reported data	–0.262	.001	0.079
Social interaction			
Device use	0.188	.045	0.093
Self-reported data	–0.030	.74	0.092
Device use			
Self-reported data	–0.218	.02	0.093

Table 7. Results of comparison of privacy concerns across data stages.

Stage (I) and stage (J)	Mean difference (I–J)	*P* value	SE
Collect			
Store	–0.056	.36	0.060
Transmit	–0.197	.01	0.075
Share	–0.336	<.001	0.091
Store			
Transmit	–0.142	.01	0.057
Share	–0.281	<.001	0.068
Transmit			
Share	–0.139	.02	0.061

The analysis results of data stage show that the data transmission stage raises greater privacy concerns than both data collection (P=.01) and data storage stages (P=.01), whereas the data sharing stage also raises higher privacy concerns than the data collection (P<.001), data storage (P<.001), and data transmission stages (P=.02). However, no difference was detected between the data collection and data storage stages (P=.36). Thus, hypotheses 1, 2.1 (i), 2.1 (ii), 2.2 (i), and 2.2 (ii) are supported.

Effects on Continuous Usage Intention

The results of PLS regression analysis are reported in Table 8 and Figure 2. The results show that privacy victimization experience (P=.01) has a significant effect, whereas privacy awareness has a marginally significant effect (P=.08) on privacy concerns. Therefore, hypothesis 3 is marginally supported, whereas hypothesis 4 is supported. In addition, both privacy concerns (P=.001) and HIPAA knowledge level (P<.001) have a positive effect on agreeable attitude toward privacy protection. Therefore, both hypotheses 5 and 6 are supported. Furthermore, both agreeable attitude toward privacy protection (P=.001) and MMH literacy (P=.001) have a positive effect on the continuous usage intention of MMHS. Therefore, hypotheses 7 and 8 are also supported.

Table 8. Results of partial least squares regression analysis.

Hypotheses	Estimate (SD)	t-statistic (*df*)	*P* value
Data type→Privacy concerns	—[a]	—[a]	—[a]
Data transmission and data sharing stages→Privacy concerns	—[b]	—[b]	—[b]
Privacy awareness→Privacy concerns	0.309 (0.179)	1.728 (499)	.08
Privacy victimization experience→Privacy concerns	0.434 (0.172)	2.515 (499)	.01
Privacy concerns→Agreeable attitude toward privacy protection	0.374 (0.109)	3.440 (499)	.001
HIPAA[c] knowledge level→Agreeable attitude toward privacy protection	0.422 (0.089)	4.728 (499)	<.001
Agreeable attitude toward privacy protection→Continuous usage intention of MMHS[d]	0.372 (0.116)	3.199 (499)	.001
MMH[e] literacy→Continuous usage intention of MMHS	0.370 (0.107)	3.461 (499)	.001

[a]See Table 6.

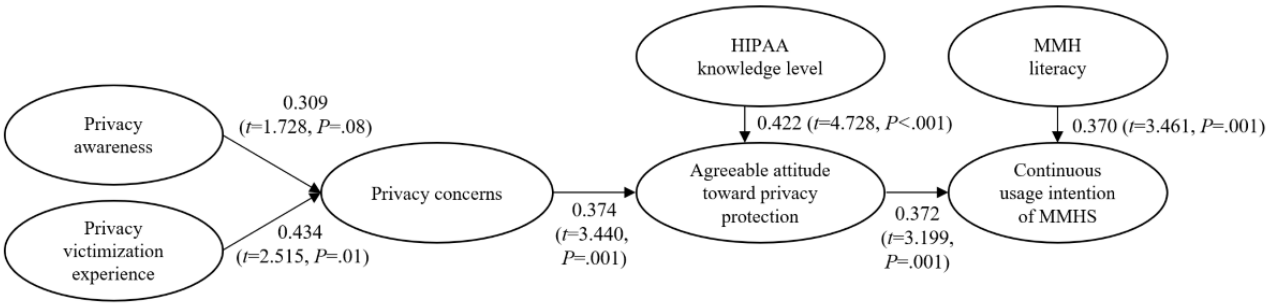
[b]See Table 7.

[c]HIPAA: Health Insurance Portability and Accountability Act.

[d]MMHS: mobile mental health systems.

[e]MMH: mobile mental health.

Figure 2. Results of the research model. HIPAA: Health Insurance Portability and Accountability Act; MMH: mobile mental health; MMHS: mobile mental health systems.



Discussion

Overview

MMHS have been increasingly used to monitor users' emotional status, improve mental illness management, and retain psychological well-being [120]. However, users' privacy concerns with regard to the use of MMHS can be a critical barrier to their adoption of, and benefiting from, these systems [121]. This study proposes and tests a novel research model for explaining user privacy concerns about MMHS from the data and user experience perspectives and examines the direct or indirect effects of privacy concerns on user perceptions of different privacy protection methods and intention to continue using MMHS.

Principal Findings

First, we discovered a significant main effect of data type on privacy concerns. Respondents expressed stronger privacy concerns about social interaction data (eg, outgoing or incoming phone calls and SMS text messages) and self-reported data (eg, current medication) than physiological data and device use data. The strong concern about social interaction data is somewhat surprising because one may assume intuitively that physiological signals (ie, skin temperature and heart rate) and physical activities (ie, walking and sleeping) should be more privacy sensitive. A possible explanation is that social isolation is one of the most typical characteristics of individuals with mental health issues [122,123]. As a result, this subpopulation may perceive social interaction data as more private than physiological and physical activity data.

Second, this study reveals a significant effect of data stage on privacy concerns. Specifically, data transmission and data sharing cause higher privacy concerns than data collection and data storage, which supports our hypotheses.

Third, the results confirm our hypothesis that privacy victimization experience has a positive effect on privacy concerns. Although privacy awareness is positively associated with privacy concerns, this effect was only marginally significant at a 0.1 significance level. A possible explanation lies in what constitutes privacy awareness. Correia and Compeau [124] argue that privacy awareness consists of 3 elements: the literacy of the elements related to privacy, the recognition that the elements exist in a current system, and the forecast of their impacts on the future. Thus, these aspects may guide future efforts in improving the effectiveness of privacy awareness training.

Fourth, the findings of this study show that increasing privacy concerns escalate agreeable attitude toward privacy protection.

Fifth, our findings show that privacy knowledge about HIPAA contributes to an agreeable attitude toward privacy protection of MMHS. In addition, MMH literacy facilitates continuous usage intention of using MMHS. The findings suggest the importance of increasing privacy knowledge and mHealth literacy of users with mental health issues for improving the use of MMHS.

Research Contributions

Despite increasing efforts being made with regard to leveraging mobile and sensing technologies for improving public mental health, there has been a lack of research on the understanding of users' privacy concerns and their impacts on the use of MMHS. This study makes contributions to the multidisciplinary literature. First, to the best of our knowledge, this study is the first research effort that systematically investigates user privacy concerns in the context of MMHS. Second, this study not only extends the Antecedents→Privacy Concerns→Outcomes model to MMHS, but also introduces new constructs, including HIPAA knowledge level and MMH literacy. Third, unlike prior studies that treated privacy data as monotonic [86,125,126], this research for the first time innovatively probes different data types and stages while investigating privacy concerns. The differences in the effects on privacy concerns of different data types and data stages have significant implications for future privacy research. Fourth, this study introduces MMH literacy as an antecedent to the continuous usage intention of MMHS. eHealth literacy has been used to assess healthy behavior on the internet [127-129], but it has rarely been used to explain the continuous intention to use innovative technology. Last but not least, this study goes beyond privacy concerns by understanding their effects on privacy protection. Our research findings reveal that an agreeable attitude toward privacy protection mediates the relationship between privacy concerns and users' continuous MMHS usage intention.

Practical Implications

This study offers a number of practical implications for different stakeholders of MMHS. For designers and developers of user-centric privacy-protecting MMHS, different effects of various personal data on privacy concerns suggest that different types of personal data should not be treated equally from a privacy protection perspective; designers and developers should care not only about the types of user data being collected, but also about how the data will be processed. In particular, they should pay more attention to effective privacy protection methods deployed for data sharing and data transmission than those deployed for data collection and data storage. As users differ in terms of their sensitivity to privacy and different personal data, the deployed privacy protection methods should be user-centered and personalized; the effect of privacy concerns on continuous MMHS usage intention can be mediated by privacy protection. Thus, implementing privacy protection measures and developing ways to improve the MMH literacy of patients can be effective strategies for increasing the trust of patients with mental health issues in MMHS and their adoption and continuous use of MMHS.

From an MMHS user perspective, users should increase their awareness of different types of data collected by MMHS; improve their knowledge regarding privacy and MMH literacy; and be educated about different privacy protection methods, which can help them choose MMHS and understand how these methods can possibly address their privacy concerns.

The following is a set of general guidelines for the design of user-centered, privacy-preserving MMHS based on the findings of this research:

- Only collect user data that are relevant to MMH
- Deidentify any data that may reveal the identity of individual users
- Encrypt data, particularly during data transmission and data sharing
- Provide user-controlled data collection, enabling users to remove certain collected data of their choice
- Provide user-controlled data access: data access and sharing should be limited to specific, user-approved parties
- Provide continuous mobile user authentication to ensure that the data are collected from the right person
- Include audits and risk assessment in privacy protocols
- Set up a policy that encrypts self-reported data and social interaction data
- Collect information about users' prior experiences of privacy victimization and recommend targeted privacy protection methods
- Improve public education about the goals, methods, and procedures of data management and privacy protection, which is essential
- Allow users to adjust privacy levels and retract collected data. This will be one of the balanced solutions in practice
- Design MMHS with an emphasis on personalized privacy protection. Personalization is one of the key features of recent MMHS to provide customized treatment to individuals

Limitations of the Study and Future Research

This study includes several limitations that offer future research opportunities. We used a web-based survey for data collection in this study, which is subject to the limitations of self-reported data. Future studies may collect actual patient use data by either collaborating with MMHS providers or using self-developed mobile apps. We also acknowledge that our recruitment strategy may pose a potential risk for selection bias—though our university-wide solicitation for participation was circulated through the university's email listserv, students could be more technology savvy and therefore more willing to participate than faculty and staff members. In addition, our recruitment flyer, which was circulated through online mental health communities, may have caused hesitation among individuals who have privacy concerns about using technology for mental health to participate in this survey. In addition to data type and data stage, other factors of MMHS, such as system functions, can be potential antecedents of privacy concerns. For instance, MMHS that focus on improving mindfulness and sleep quality, such as Calm and Headspace [130,131], are likely to yield different levels of privacy concerns compared with MMHS that focus on serious

clinical mental illness, such as PTSD Coach and NOCD (an MMHS for the treatment of obsessive-compulsive disorder).

Acknowledgments

This research was sponsored in part by the US National Science Foundation (award number: CNS 1704800) and the University of North Carolina at Charlotte School of Data Science Seed Grant (award number 2020005). Any opinions, findings, and conclusions expressed in this manuscript are those of the authors and do not necessarily reflect the views of the sponsors.

Conflicts of Interest

None declared.

Multimedia Appendix 1

A summary of collected patient data and privacy protection methods in existing mobile mental health studies (N=32).
[DOCX File , 22 KB-Multimedia Appendix 1]

Multimedia Appendix 2

Survey questionnaire.
[DOCX File , 23 KB-Multimedia Appendix 2]

Multimedia Appendix 3

Construct measurement - privacy concerns.
[DOCX File , 17 KB-Multimedia Appendix 3]

Multimedia Appendix 4

Construct measurements - other concerns.
[DOCX File , 19 KB-Multimedia Appendix 4]

Multimedia Appendix 5

Correlations among the constructs.
[DOCX File , 14 KB-Multimedia Appendix 5]

Multimedia Appendix 6

Discriminant validity: Heterotrait-Monotrait ratio of correlations.
[DOCX File , 13 KB-Multimedia Appendix 6]

Multimedia Appendix 7

Factor loadings.
[DOCX File , 18 KB-Multimedia Appendix 7]

References

1. Kotz D, Gunter CA, Kumar S, Weiner JP. Privacy and security in mobile health: a research agenda. Computer (Long Beach Calif) 2016 Jun;49(6):22-30 [FREE Full text] [doi: 10.1109/MC.2016.185] [Medline: 28344359]
2. Silver L. Smartphone ownership is growing rapidly around the world, but not always equally. Pew Research Center. 2019. URL: https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/ [accessed 2021-11-15]
3. Islam MA, Choudhury N. Mobile apps for mental health: a content analysis. Indian J Mental Health 2020;7(3):222-229 [FREE Full text]
4. Bidja P. DepressionGNN: depression prediction using graph neural network on smartphone and wearable sensors. University of Connecticut. 2019. URL: https://opencommons.uconn.edu/cgi/viewcontent.cgi?article=1640&context=srhonors_theses [accessed 2021-11-09]
5. Cao B, Zheng L, Zhang C, Yu PS, Piscitello A, Zulueta J, et al. DeepMood: modeling mobile phone typing dynamics for mood detection. In: Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2017 Presented at: Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining; Aug 13 - 17, 2017; Halifax NS Canada. [doi: 10.1145/3097983.3098086]

6. Wang R, Wang W, Aung MS, Ben-Zeev D, Brian R, Campbell AT, et al. Predicting symptom trajectories of schizophrenia using mobile sensing. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 2017 Sep;1(3):1-24 [FREE Full text] [doi: 10.1145/3130976]
7. Smith HJ, Dinev T, Xu H. Information privacy research: an interdisciplinary review. MIS Q 2011 Dec;35(4):989-1015. [doi: 10.2307/41409970]
8. Privacy and confidentiality in the nationwide health information network. National Committee on Vital and Health Statistics. URL: https://library.ahima.org/doc?oid=75960#.YZKBzGBBzIU [accessed 2021-11-15]
9. Arora S, Yttri J, Nilse W. Privacy and security in mobile health (mHealth) research. Alcohol Res 2014;36(1):143-151 [FREE Full text] [Medline: 26259009]
10. Sampat BH, Prabhakar B. Privacy risks and security threats in mHealth apps. J Int Technol Inf Manag 2017;26(4):126-153 [FREE Full text]
11. Tovino SA. Privacy and security issues with mobile health research applications. J Law Med Ethics 2020 Mar;48(1_suppl):154-158. [doi: 10.1177/1073110520917041] [Medline: 32342741]
12. Birenboim A, Dijst M, Scheepers FE, Poelman MP, Helbich M. Wearables and location tracking technologies for mental-state sensing in outdoor environments. Prof Geogr 2019 Mar 25;71(3):449-461. [doi: 10.1080/00330124.2018.1547978]
13. Salafi T, Kah J. Design of unobtrusive wearable mental stress monitoring device using physiological sensor. In: 7th WACBE World Congress on Bioengineering 2015. Cham: Springer; 2015.
14. Bogomolov A, Lepri B, Ferron M, Pianesi F, Pentland A. Daily stress recognition from mobile phone data, weather conditions and individual traits. In: Proceedings of the 22nd ACM International Conference on Multimedia. 2014 Presented at: Proceedings of the 22nd ACM international conference on Multimedia; Nov 3 - 7, 2014; Orlando Florida USA. [doi: 10.1145/2647868.2654933]
15. Kidd SA, Feldcamp L, Adler A, Kaleis L, Wang W, Vichnevetski K, et al. Feasibility and outcomes of a multi-function mobile health approach for the schizophrenia spectrum: App4Independence (A4i). PLoS One 2019;14(7):e0219491 [FREE Full text] [doi: 10.1371/journal.pone.0219491] [Medline: 31306439]
16. Meyer N, Kerz M, Folarin A, Joyce DW, Jackson R, Karr C, et al. Capturing rest-activity profiles in schizophrenia using wearable and mobile technologies: development, implementation, feasibility, and acceptability of a remote monitoring platform. JMIR Mhealth Uhealth 2018 Oct 30;6(10):e188 [FREE Full text] [doi: 10.2196/mhealth.8292] [Medline: 30377146]
17. Fraiwan L, Basmaji T, Hassanin O. A mobile mental health monitoring system: a smart glove. In: Proceedings of the 2018 14th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS). 2018 Presented at: 2018 14th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS); Nov 26-29, 2018; Las Palmas de Gran Canaria, Spain. [doi: 10.1109/sitis.2018.00043]
18. Yang S, Gao B, Jiang L, Jin J, Gao Z, Ma X, et al. IoT structured long-term wearable social sensing for mental wellbeing. IEEE Internet Things J 2019 Apr;6(2):3652-3662. [doi: 10.1109/jiot.2018.2889966]
19. Abdullah S, Matthews M, Frank E, Doherty G, Gay G, Choudhury T. Automatic detection of social rhythms in bipolar disorder. J Am Med Inform Assoc 2016 May;23(3):538-543. [doi: 10.1093/jamia/ocv200] [Medline: 26977102]
20. Barth S, de Jong MD. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. Telemat Inf 2017 Nov;34(7):1038-1058. [doi: 10.1016/j.tele.2017.04.013]
21. Acquisti A, Adjerid I, Balebako R, Brandimarte L, Cranor LF, Komanduri S, et al. Nudges for privacy and security. ACM Comput Surv 2017 Oct;50(3):1-41. [doi: 10.1145/3054926]
22. Caine K. Exploring everyday privacy behaviors and misclosures. Georgia Tech Library. 2009. URL: https://smartech.gatech.edu/handle/1853/31665?show=full [accessed 2021-11-15]
23. Zhou L, Bao J, Watzlaf V, Parmanto B. Barriers to and facilitators of the use of mobile health apps from a security perspective: mixed-methods study. JMIR Mhealth Uhealth 2019 Apr 16;7(4):e11223 [FREE Full text] [doi: 10.2196/11223] [Medline: 30990458]
24. Culnan MJ, Armstrong PK. Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organ Sci 1999 Feb;10(1):104-115. [doi: 10.1287/orsc.10.1.104]
25. Warren SD, Brandeis LD. The right to privacy. Harv Law Rev 1890 Dec 15;4(5):193-220. [doi: 10.2307/1321160]
26. Kweon H, Zhang D, Zhou L, editors. Privacy in Mobile Advertising: From a User Perspective. 2012 Aug Presented at: 18th Americas Conference on Information Systems; 2012; Seattle, USA.
27. Crossler R, Bélanger F. The mobile privacy-security knowledge gap model: understanding behaviors. CORE. URL: https://core.ac.uk/download/pdf/77239956.pdf [accessed 2021-11-15]
28. Kokolakis S. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Comput Secur 2017 Jan;64:122-134. [doi: 10.1016/j.cose.2015.07.002]
29. Plachkinova M, Andrés S, Chatterjee S. A taxonomy of mhealth apps - security and privacy concerns. In: Proceedings of the 2015 48th Hawaii International Conference on System Sciences. 2015 Presented at: 2015 48th Hawaii International Conference on System Sciences; Jan 5-8, 2015; Kauai, HI, USA. [doi: 10.1109/hicss.2015.385]
30. Stavrou E, Pitsillides A. Security challenges in a mobile healthcare environment. In: Proceedings of the IWWST '05, 3rd International Workshop in Wireless Security Technologies. 2005 Presented at: IWWST '05, 3rd International Workshop in Wireless Security Technologies; Apr 4-5, 2005; London, UK.

31. Kotz D. A threat taxonomy for mHealth privacy. In: Proceedings of the 2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011). 2011 Presented at: 2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011); Jan 4-8, 2011; Bangalore, India. [doi: 10.1109/comsnets.2011.5716518]
32. Armontrout J, Torous J, Fisher M, Drogin E, Gutheil T. Mobile mental health: navigating new rules and regulations for digital tools. Curr Psychiatry Rep 2016 Oct 23;18(10):91. [doi: 10.1007/s11920-016-0726-x] [Medline: 27553979]
33. Ohno-Machado L, Wang S, Wang X, Iranmehr A, Jiang X. Privacy, security, and machine learning for mobile health applications. American Association for the Advancement of Science. URL: https://www.aaas.org/sites/default/files/Ohno%20Privacy,%20Security,%20and%20Machine%20Learning%20for%20Mobile%20Health%20Applications%20.pdf [accessed 2021-11-15]
34. Proposed Revisions to the Common Rule for the Protection of Human Subjects in the Behavioral and Social Sciences. Washington (DC): National Academies Press (US); 2014.
35. Ray S, Biswas G. Design of an efficient mobile health system for achieving HIPAA privacy-security regulations. Int J Wireless Mobile Comput 2014;7(4):378-387. [doi: 10.1504/ijwmc.2014.063056]
36. Xcertia mHealth app guidelines. Xcertia Guidelines. 2019. URL: https://www.himss.org/sites/hde/files/media/file/2020/04/17/xcertia-guidelines-2019-final.pdf [accessed 2021-11-09]
37. Bardram JE, Matic A. A decade of ubiquitous computing research in mental health. IEEE Pervasive Comput 2020 Jan;19(1):62-72. [doi: 10.1109/mprv.2019.2925338]
38. Tsiouris KM, Gatsios D, Rigas G, Miljkovic D, Koroušić Seljak B, Bohanec M, et al. PD_Manager: an mHealth platform for Parkinson's disease patient management. Healthc Technol Lett 2017 Jun;4(3):102-108 [FREE Full text] [doi: 10.1049/htl.2017.0007] [Medline: 28706727]
39. Arroyo-Gallego T, Ledesma-Carbayo MJ, Sanchez-Ferro A, Butterworth I, Mendoza CS, Matarazzo M, et al. Detection of Motor Impairment in Parkinson's Disease Via Mobile Touchscreen Typing. IEEE Trans Biomed Eng 2017 Sep;64(9):1994-2002. [doi: 10.1109/TBME.2017.2664802] [Medline: 28237917]
40. Bitsaki M, Koutras C, Koutras G, Leymann F, Steimle F, Wagner S, et al. ChronicOnline: implementing a mHealth solution for monitoring and early alerting in chronic obstructive pulmonary disease. Health Informatics J 2017 Sep;23(3):197-207 [FREE Full text] [doi: 10.1177/1460458216641480] [Medline: 27102885]
41. Saeb S, Lattie EG, Schueller SM, Kording KP, Mohr DC. The relationship between mobile phone location sensor data and depressive symptom severity. PeerJ 2016 Sep 29;4:e2537 [FREE Full text] [doi: 10.7717/peerj.2537] [Medline: 28344895]
42. Saeb S, Zhang M, Kwasny MM, Karr CJ, Kording K, Mohr DC. The Relationship between Clinical, Momentary, and Sensor-based Assessment of Depression. Int Conf Pervasive Comput Technol Healthc 2015 Aug;2015 [FREE Full text] [doi: 10.4108/icst.pervasivehealth.2015.259034] [Medline: 26640739]
43. Delahunty F, Wood I, Arcan M. First insights on a passive major depressive disorder prediction system with incorporated conversational chatbot. In: Proceedings of the Irish Conference on Artificial Intelligence and Cognitive Science. 2018 Presented at: Irish Conference on Artificial Intelligence and Cognitive Science; Aug 19-21, 2009; Dublin, Ireland URL: https://repository.ust.hk/ir/Record/1783.1-95166 [doi: 10.1007/978-3-642-17080-5]
44. Alvarez-Lozano J, Osmani V, Mayora O, Frost M, Bardram J, Faurholt-Jepsen M. Tell me your apps and I will tell you your mood: correlation of apps usage with bipolar disorder state. In: Proceedings of the 7th International Conference on PErvasive Technologies Related to Assistive Environments. 2014 May Presented at: Proceedings of the 7th International Conference on Pervasive Technologies Related to Assistive Environments; May 27 - 30, 2014; Rhodes Greece URL: https://dl.acm.org/doi/10.1145/2674396.2674408 [doi: 10.1145/2674396.2674408]
45. Grünerbl A, Muaremi A, Osmani V, Bahle G, Ohler S, Tröster G, et al. Smartphone-based recognition of states and state changes in bipolar disorder patients. IEEE J Biomed Health Inform 2015 Jan;19(1):140-148. [doi: 10.1109/JBHI.2014.2343154] [Medline: 25073181]
46. Faurholt-Jepsen M, Vinberg M, Frost M, Christensen EM, Bardram JE, Kessing LV. Smartphone data as an electronic biomarker of illness activity in bipolar disorder. Bipolar Disord 2015 Nov;17(7):715-728. [doi: 10.1111/bdi.12332] [Medline: 26395972]
47. Wang R, Aung M, Abdullah S, Brian R, Campbell A, Choudhury T. CrossCheck: toward passive sensing and detection of mental health changes in people with schizophrenia. In: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing. 2016 Presented at: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing; Sep 12 - 16, 2016; Heidelberg Germany URL: https://www.semanticscholar.org/paper/CrossCheck%3A-toward-passive-sensing-and-detection-of-Wang-Aung/0298d6c953f9b04f557687f276430afa750a1766 [doi: 10.1145/2971648.2971740]
48. Ben-Zeev D, Wang R, Abdullah S, Brian R, Scherer EA, Mistler LA, et al. Mobile behavioral sensing for outpatients and inpatients with Schizophrenia. Psychiatr Serv 2016 May 01;67(5):558-561 [FREE Full text] [doi: 10.1176/appi.ps.201500130] [Medline: 26695497]
49. Sano A, Phillips AJ, Yu AZ, McHill AW, Taylor S, Jaques N, et al. Recognizing academic performance, sleep quality, stress level, and mental health using personality traits, wearable sensors and mobile phones. Int Conf Wearable Implant Body Sens Netw 2015 Jun;2015:- [FREE Full text] [doi: 10.1109/BSN.2015.7299420] [Medline: 28516162]

50. Naddeo S, Verde L, Forastiere M, De Pietro G, Sannino G. A real-time m-health monitoring system: an integrated solution combining the use of several wearable sensors and mobile devices. In: Proceedings of the 10th International Joint Conference on Biomedical Engineering Systems and Technologies. 2017 Presented at: Proceedings of the 10th International Joint Conference on Biomedical Engineering Systems and Technologies; Feb21-23, 2017; Porto, Portugal. [doi: 10.5220/0006296105450552]
51. Lanata A, Valenza G, Nardelli M, Gentili C, Scilingo EP. Complexity index from a personalized wearable monitoring system for assessing remission in mental health. IEEE J Biomed Health Inform 2015 Jan;19(1):132-139. [doi: 10.1109/JBHI.2014.2360711] [Medline: 25291802]
52. Boonstra TW, Nicholas J, Wong QJ, Shaw F, Townsend S, Christensen H. Using mobile phone sensor technology for mental health research: integrated analysis to identify hidden challenges and potential solutions. J Med Internet Res 2018 Jul 30;20(7):e10131 [FREE Full text] [doi: 10.2196/10131] [Medline: 30061092]
53. Zulueta J, Piscitello A, Rasic M, Easter R, Babu P, Langenecker SA, et al. Predicting mood disturbance severity with mobile phone keystroke metadata: a biaffect digital phenotyping study. J Med Internet Res 2018 Jul 20;20(7):e241 [FREE Full text] [doi: 10.2196/jmir.9775] [Medline: 30030209]
54. Ko C, Leu F, Lin I. A wandering path tracking and fall detection system for people with dementia. In: Proceedings of the 2014 Ninth International Conference on Broadband and Wireless Computing, Communication and Applications. 2014 Presented at: International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA); Nov 8-10, 2014; Guangdong, China. [doi: 10.1109/bwcca.2014.127]
55. Dolatabadi E, Zhi YX, Flint AJ, Mansfield A, Iaboni A, Taati B. The feasibility of a vision-based sensor for longitudinal monitoring of mobility in older adults with dementia. Arch Gerontol Geriatr 2019;82:200-206. [doi: 10.1016/j.archger.2019.02.004] [Medline: 30831526]
56. Sano A, Taylor S, McHill AW, Phillips AJ, Barger LK, Klerman E, et al. Identifying objective physiological markers and modifiable behaviors for self-reported stress and mental health status using wearable sensors and mobile phones: observational study. J Med Internet Res 2018 Jun 08;20(6):e210 [FREE Full text] [doi: 10.2196/jmir.9410] [Medline: 29884610]
57. Vildjiounaite E, Kallio J, Kyllönen V, Nieminen M, Määttänen I, Lindholm M, et al. Unobtrusive stress detection on the basis of smartphone usage data. Pers Ubiquitous Comput 2018 Jan 17;22(4):671-688. [doi: 10.1007/s00779-017-1108-z]
58. Voss C, Schwartz J, Daniels J, Kline A, Haber N, Washington P, et al. Effect of wearable digital intervention for improving socialization in children with autism spectrum disorder: a randomized clinical trial. JAMA Pediatr 2019 May 01;173(5):446-454 [FREE Full text] [doi: 10.1001/jamapediatrics.2019.0285] [Medline: 30907929]
59. Nurgalieva L, O'Callaghan D, Doherty G. Security and privacy of mHealth applications: a scoping review. IEEE Access 2020;8:104247-104268. [doi: 10.1109/access.2020.2999934]
60. O'Loughlin K, Neary M, Adkins EC, Schueller SM. Reviewing the data security and privacy policies of mobile apps for depression. Internet Interv 2019 Mar;15:110-115 [FREE Full text] [doi: 10.1016/j.invent.2018.12.001] [Medline: 30792962]
61. Bella G, Coles-Kemp L. Internet users' security and privacy while they interact with Amazon. In: Proceedings of the 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications. 2011 Presented at: 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications; Changsha; Nov 16-18, 2011. [doi: 10.1109/trustcom.2011.118]
62. Xie W, Karan K. Consumers' privacy concern and privacy protection on social network sites in the era of big data: empirical evidence from college students. J Interact Advert 2019 Sep 04;19(3):187-201. [doi: 10.1080/15252019.2019.1651681]
63. Metzger M. Communication privacy management in electronic commerce. J Comput Mediat Commun 2007;12(2):335-361. [doi: 10.1111/j.1083-6101.2007.00328.x]
64. Prince C. Do consumers want to control their personal data? Empirical evidence. Int J Hum Comput Stud 2018 Feb;110:21-32. [doi: 10.1016/j.ijhcs.2017.10.003]
65. Houghton DJ, Joinson AN. Privacy, social network sites, and social relations. J Technol Hum Serv 2010 May 10;28(1-2):74-94. [doi: 10.1080/15228831003770775]
66. Jin SAA. Peeling back the multiple layers of Twitter's private disclosure onion: the roles of virtual identity discrepancy and personality traits in communication privacy management on Twitter. New Media Soc 2013 Feb 07;15(6):813-833. [doi: 10.1177/1461444812471814]
67. Xu Z. An empirical study of patients' privacy concerns for health informatics as a service. Technol Forecast Soc Change 2019 Jun;143:297-306. [doi: 10.1016/j.techfore.2019.01.018]
68. Hindy H, Brosset D, Bayne E, Seeam AK, Tachtatzis C, Atkinson R, et al. A taxonomy of network threats and the effect of current datasets on intrusion detection systems. IEEE Access 2020;8:104650-104675. [doi: 10.1109/access.2020.3000179]
69. Zeissig E, Lidynia C, Vervier L, Gadeib A, Ziefle M. Online privacy perceptions of older adults. In: International Conference on Human Aspects of IT for the Aged Population. Cham: Springer; 2017.
70. Malhotra NK, Kim SS, Agarwal J. Internet Users' Information Privacy Concerns (IUIPC): the construct, the scale, and a causal model. Inf Syst Res 2004 Dec;15(4):336-355. [doi: 10.1287/isre.1040.0032]
71. Mamonov S, Benbunan-Fich R. The impact of information security threat awareness on privacy-protective behaviors. Comput Hum Behav 2018 Jun;83:32-44. [doi: 10.1016/j.chb.2018.01.028]

72. Ozdemir ZD, Jeff Smith H, Benamati JH. Antecedents and outcomes of information privacy concerns in a peer context: an exploratory study. Eur J Inf Syst 2018 Feb 15;26(6):642-660. [doi: 10.1057/s41303-017-0056-z]
73. Widjaja AE, Chen JV, Sukoco BM, Ha QA. Understanding users' willingness to put their personal information on the personal cloud-based storage applications: an empirical study. Comput Human Behav 2019 Feb;91:167-185. [doi: 10.1016/j.chb.2018.09.034]
74. Shipman F, Marshall C. Ownership, privacy, and control in the wake of Cambridge analytica: the relationship between attitudes and awareness. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 2020 Presented at: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems; Apr 25-30, 2020; Honolulu. [doi: 10.1145/3313831.3376662]
75. Bansal G, Zahedi FM, Gefen D. Do context and personality matter? Trust and privacy concerns in disclosing private information online. Inf Manag 2016 Jan;53(1):1-21. [doi: 10.1016/j.im.2015.08.001]
76. Xu H, Gupta S, Rosson M, Carroll J. Measuring Mobile Users' Concerns for Information Privacy. USA: ICIS; 2012.
77. Chen H, Beaudoin CE, Hong T. Securing online privacy: an empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. Comput Hum Behav 2017 May 27;70(1):291-302 [FREE Full text] [doi: 10.1016/j.chb.2017.01.003]
78. Green B, Gies S, Bobnis A, Piquero NL, Piquero AR, Velasquez E. The role of victim services for individuals who have experienced serious identity-based crime. Victim Offender 2020 Apr 14;15(6):720-743. [doi: 10.1080/15564886.2020.1743804]
79. Hong W, Chan F, Thong J. Drivers and inhibitors of internet privacy concern: a multidimensional development theory perspective. J Bus Ethics 2019 Jun 17;168(3):539-564. [doi: 10.1007/s10551-019-04237-1]
80. Kumar S, Kumar P, Bhasker B. Interplay between trust, information privacy concerns and behavioural intention of users on online social networks. Behav Inf Technol 2018 May 09;37(6):622-633. [doi: 10.1080/0144929x.2018.1470671]
81. Kim S, Park H, Choi MJ. Negative impact of social network services based on stressor-stress-outcome: the role of experience of privacy violations. Future Internet 2019 Jun 20;11(6):137. [doi: 10.3390/fi11060137]
82. Degirmenci K. Mobile users' information privacy concerns and the role of app permission requests. Int J Inf Manag 2020 Feb;50:261-272. [doi: 10.1016/j.ijinfomgt.2019.05.010]
83. Gu J, Xu Y, Xu H, Zhang C, Ling H. Privacy concerns for mobile app download: an elaboration likelihood model perspective. Decis Support Syst 2017 Feb;94:19-28. [doi: 10.1016/j.dss.2016.10.002]
84. Kraus L, Wechsung I, Möller S. A comparison of privacy and security knowledge and privacy concern as influencing factors for mobile protection behavior. In: Proceedings of the Workshop on Privacy Personas and Segmentation. 2014 Presented at: Workshop on Privacy Personas and Segmentation; Jul 9-11, 2014; Menlo Park, CA.
85. Alshammari N, Mylonas A, Sedky M, Champion J, Bauer C. Exploring the adoption of physical security controls in smartphones. In: International Conference on Human Aspects of Information Security, Privacy, and Trust. Cham: Springer; 2015.
86. Boerman SC, Kruikemeier S, Zuiderveen Borgesius FJ. Exploring motivations for online privacy protection behavior: insights from panel data. Commun Res 2018 Oct 05;48(7):953-977. [doi: 10.1177/0093650218800915]
87. Saeri AK, Ogilvie C, La Macchia ST, Smith JR, Louis WR. Predicting Facebook users' online privacy protection: risk, trust, norm focus theory, and the theory of planned behavior. J Soc Psychol 2014;154(4):352-369. [doi: 10.1080/00224545.2014.914881] [Medline: 25154118]
88. Gao W, Liu Z, Guo Q, Li X. The dark side of ubiquitous connectivity in smartphone-based SNS: an integrated model from information perspective. Comput Hum Behav 2018 Jul;84:185-193. [doi: 10.1016/j.chb.2018.02.023]
89. Anic I, Škare V, Kursan Milaković I. The determinants and effects of online privacy concerns in the context of e-commerce. Electron Commer Res Appl 2019;36:100868. [doi: 10.1016/j.elerap.2019.100868]
90. Beaver K, Barnes J, Boutwell B. The Nurture Versus Biosocial Debate in Criminology: On the Origins of Criminal Behavior and Criminality. Thousand Oaks, California: SAGE Publications; 2014.
91. Norman P, Boer H, Seydel E. Protection motivation theory. In: Predicting Health Behaviour: Research and Practice With Social Cognition Models. Berkshire: Open University Press; 2005.
92. Rogers R, Prentice-Dunn S. Protection motivation theory. In: Handbook of Health Behavior Research 1: Personal and Social Determinants. New York: Plenum Press; 1997.
93. Alanazi MH, Soh B. Behavioral intention to use IoT technology in healthcare settings. Eng Technol Appl Sci Res 2019 Oct 09;9(5):4769-4774. [doi: 10.48084/etasr.3063]
94. Wendel S, Dellaert BG, Ronteltap A, van Trijp HC. Consumers' intention to use health recommendation systems to receive personalized nutrition advice. BMC Health Serv Res 2013 Apr 04;13:126 [FREE Full text] [doi: 10.1186/1472-6963-13-126] [Medline: 23557363]
95. Lebek B, Degirmenci K, Breitner M. Investigating the influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices. In: Proceedings of the 19th Americas Conference on Information Systems, AMCIS 2013. 2013 Presented at: 19th Americas Conference on Information Systems, AMCIS 2013; Aug 15-17, 2013; Chicago, Illinois, USA.

96. Noblin AM, Wan TT, Fottler M. The impact of health literacy on a patient's decision to adopt a personal health record. Perspect Health Inf Manag 2012 Oct 1;9:1-13 [FREE Full text] [Medline: 23209454]
97. Norman CD, Skinner HA. eHEALS: the eHealth literacy scale. J Med Internet Res 2006 Nov 14;8(4):e27 [FREE Full text] [doi: 10.2196/jmir.8.4.e27] [Medline: 17213046]
98. Zhang X, Yan X, Cao X, Sun Y, Chen H, She J. The role of perceived e-health literacy in users' continuance intention to use mobile healthcare applications: an exploratory empirical study in China. Inf Technol Dev 2017 Mar 09;24(2):198-223. [doi: 10.1080/02681102.2017.1283286]
99. Petty RE, Cacioppo JT, Goldman R. Personal involvement as a determinant of argument-based persuasion. J Pers Soc Psychol 1981 Nov;41(5):847-855. [doi: 10.1037/0022-3514.41.5.847]
100. Britt RK, Collins WB, Wilson K, Linnemeier G, Englebert AM. eHealth literacy and health behaviors affecting modern college students: a pilot study of issues identified by the american college health association. J Med Internet Res 2017 Dec 19;19(12):e392 [FREE Full text] [doi: 10.2196/jmir.3100] [Medline: 29258979]
101. Kim EJ, Yu JH, Kim EY. Pathways linking mental health literacy to professional help-seeking intentions in Korean college students. J Psychiatr Ment Health Nurs 2020 Aug;27(4):393-405. [doi: 10.1111/jpm.12593] [Medline: 31954091]
102. Fox G, James TL. Toward an understanding of the antecedents to health information privacy concern: a mixed methods study. Inf Syst Front 2020 Aug 21:1-26. [doi: 10.1007/s10796-020-10053-0]
103. Zhang X, Liu S, Chen X, Wang L, Gao B, Zhu Q. Health information privacy concerns, antecedents, and information disclosure intention in online health communities. Inf Manag 2018 Jun;55(4):482-493. [doi: 10.1016/j.im.2017.11.003]
104. Chang SE, Shen W, Liu AY. Why mobile users trust smartphone social networking services? A PLS-SEM approach. J Bus Res 2016 Nov;69(11):4890-4895. [doi: 10.1016/j.jbusres.2016.04.048]
105. Smith HJ, Milberg SJ, Burke SJ. Information privacy: measuring individuals' concerns about organizational practices. MIS Quart 1996 Jun;20(2):167. [doi: 10.2307/249477]
106. Terry NP, Gunter TD. Regulating mobile mental health apps. Behav Sci Law 2018 Mar;36(2):136-144. [doi: 10.1002/bsl.2339] [Medline: 29659069]
107. Ringle CM, Wende S, Becker JM. SmartPLS 3. Boenningstedt: SmartPLS GmbH; 2015.
108. Pedhazur E, Kerlinger F. Multiple Regression in Behavioral Research. New York: Holt, Rinehart, and Winston; 1982.
109. Slinker BK, Glantz SA. Multiple regression for physiological data analysis: the problem of multicollinearity. Am J Physiol 1985 Jul;249(1 Pt 2):R1-12. [doi: 10.1152/ajpregu.1985.249.1.R1] [Medline: 4014489]
110. Kaiser HF. The varimax criterion for analytic rotation in factor analysis. Psychometrika 1958 Sep;23(3):187-200. [doi: 10.1007/BF02289233]
111. Tavakol M, Dennick R. Making sense of Cronbach's alpha. Int J Med Educ 2011 Jun 27;2:53-55 [FREE Full text] [doi: 10.5116/ijme.4dfb.8dfd] [Medline: 28029643]
112. Fornell C, Larcker D. Structural equation models with unobservable variables and measurement error: Algebra and statistics. J Mark Res 1981 Aug;18(3):382-388. [doi: 10.2307/3150980]
113. Henseler J, Ringle CM, Sarstedt M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. J Acad Mark Sci 2014 Aug 22;43(1):115-135. [doi: 10.1007/s11747-014-0403-8]
114. Shook CL, Ketchen DJ, Hult GT, Kacmar KM. An assessment of the use of structural equation modeling in strategic management research. Strategic Manag J 2004 Apr;25(4):397-404. [doi: 10.1002/smj.385]
115. Wasil AR, Gillespie S, Schell T, Lorenzo-Luaces L, DeRubeis RJ. Estimating the real-world usage of mobile apps for mental health: development and application of two novel metrics. World Psychiatry 2021 Feb 12;20(1):137-138 [FREE Full text] [doi: 10.1002/wps.20827] [Medline: 33432761]
116. Calm homepage. Calm. URL: https://www.calm.com/ [accessed 2021-11-10]
117. Talkspace homepage. Talkspace. URL: https://www.talkspace.com [accessed 2021-11-10]
118. PTSD coach. US Department of Veterans Affairs. URL: https://mobile.va.gov/app/ptsd-coach [accessed 2021-11-10]
119. Optimism review. One Mind PsyberGuide. URL: https://onemindpsyberguide.org/apps/optimism/ [accessed 2021-11-10]
120. Lecomte T, Potvin S, Corbière M, Guay S, Samson C, Cloutier B, et al. Mobile apps for mental health issues: meta-review of meta-analyses. JMIR Mhealth Uhealth 2020 May 29;8(5):e17458 [FREE Full text] [doi: 10.2196/17458] [Medline: 32348289]
121. Benjumea J, Ropero J, Rivera-Romero O, Dorronzoro-Zubiete E, Carrasco A. Privacy assessment in mobile health apps: scoping review. JMIR Mhealth Uhealth 2020 Jul 02;8(7):e18868 [FREE Full text] [doi: 10.2196/18868] [Medline: 32459640]
122. Wang J, Lloyd-Evans B, Giacco D, Forsyth R, Nebo C, Mann F, et al. Social isolation in mental health: a conceptual and methodological review. Soc Psychiatry Psychiatr Epidemiol 2017 Dec;52(12):1451-1461 [FREE Full text] [doi: 10.1007/s00127-017-1446-1] [Medline: 29080941]
123. Ma R, Mann F, Wang J, Lloyd-Evans B, Terhune J, Al-Shihabi A, et al. The effectiveness of interventions for reducing subjective and objective social isolation among people with mental health problems: a systematic review. Soc Psychiatry Psychiatr Epidemiol 2020 Jul;55(7):839-876 [FREE Full text] [doi: 10.1007/s00127-019-01800-z] [Medline: 31741017]
124. Correia J, Compeau D. Information privacy awareness (IPA): a review of the use, definition and measurement of IPA. ScholarSpace. 2017. URL: https://scholarspace.manoa.hawaii.edu/handle/10125/41646 [accessed 2021-11-15]

125. Chen H, Beaudoin CE, Hong T. Protecting oneself online: the effects of negative privacy experiences on privacy protective behaviors. J Mass Commun Q 2016 Mar 23;93(2):409-429 [FREE Full text] [doi: 10.1177/1077699016640224]
126. Mousavi R, Chen R, Kim DJ, Chen K. Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. Decis Support Syst 2020 Aug;135:113323. [doi: 10.1016/j.dss.2020.113323]
127. Suri V, Chang YK, Majid S, Foo S. Health information literacy of senior citizens – a review. In: Information Literacy. Lifelong Learning and Digital Citizenship in the 21st Century. Cham: Springer; 2014.
128. Noblin AM, Rutherford A. Impact of health literacy on senior citizen engagement in health care IT usage. Gerontol Geriatr Med 2017;3:2333721417706300 [FREE Full text] [doi: 10.1177/2333721417706300] [Medline: 28508022]
129. Aponte J, Nokes KM. Validating an electronic health literacy scale in an older hispanic population. J Clin Nurs 2017 Sep;26(17-18):2703-2711. [doi: 10.1111/jocn.13763] [Medline: 28207962]
130. Huberty J, Green J, Glissmann C, Larkey L, Puzia M, Lee C. Efficacy of the mindfulness meditation mobile app "calm" to reduce stress among college students: randomized controlled trial. JMIR Mhealth Uhealth 2019 Jun 25;7(6):e14273 [FREE Full text] [doi: 10.2196/14273] [Medline: 31237569]
131. Wen L, Sweeney TE, Welton L, Trockel M, Katznelson L. Encouraging mindfulness in medical house staff via smartphone app: a pilot study. Acad Psychiatry 2017 Oct;41(5):646-650. [doi: 10.1007/s40596-017-0768-3] [Medline: 28795335]

Abbreviations

HIPAA: Health Insurance Portability and Accountability Act
mHealth: mobile health
MMH: mobile mental health
MMHS: mobile mental health systems
PHI: protected health information
PLS: partial least squares

Edited by G Eysenbach; submitted 28.06.21; peer-reviewed by H Hao, Q Yin; comments to author 30.07.21; revised version received 06.08.21; accepted 15.10.21; published 24.12.21

Please cite as:
Zhang D, Lim J, Zhou L, Dahl AA
Breaking the Data Value-Privacy Paradox in Mobile Mental Health Systems Through User-Centered Privacy Protection: A Web-Based Survey Study
JMIR Ment Health 2021;8(12):e31633
URL: https://mental.jmir.org/2021/12/e31633
doi: 10.2196/31633
PMID: 34951604