"That's Kind of Sus(picious)": The Comprehensiveness of Mental Health Application Users' Privacy and Security Concerns

Yi Xuan Khoo
University of Maryland, Baltimore County
Baltimore, MD, USA
ykhoo1@umbc.edu

Rachael M. Kang
University of Maryland, Baltimore County
Baltimore, MD, USA
rkang3@umbc.edu

Tera L. Reynolds
University of Maryland, Baltimore County
Baltimore, MD, USA
reynoter@umbc.edu

Helena M. Mentis
University of Maryland, Baltimore County
Baltimore, MD, USA
mentis@umbc.edu

ABSTRACT

With the increasing usage of mental health applications (MHAs), there is growing concern regarding their data privacy practices. Analyzing 437 user reviews from 83 apps, we outline users' predominant privacy and security concerns with currently available apps. We then compare those concerns to criteria from two prominent app evaluation websites – Privacy Not Included and One Mind PsyberGuide. Our findings show that MHA users have myriad data privacy and security concerns including a user's control over their own data, but these concerns do not often overlap with those of experts from evaluation websites who focus more on issues such as required password strength. We highlight this disconnect and propose solutions in how the mental health care ecosystem can provide better guidance to MHA users and experts from the fields of privacy and security and mental health technology in choosing and evaluating, respectively, potentially useful mental health apps.

CCS CONCEPTS

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

KEYWORDS

mental health, apps, privacy, security

ACM Reference Format:
Yi Xuan Khoo, Rachael M. Kang, Tera L. Reynolds, and Helena M. Mentis. 2024. "That's Kind of Sus(picious)": The Comprehensiveness of Mental Health Application Users' Privacy and Security Concerns. 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, 16 pages. https://doi.org/10.1145/3613904.3642705

1 INTRODUCTION

Since 2020, at least 4 in 10 adults in the United States have encountered significant levels of psychological distress [53]. Yet, around 40% of people who have experienced mental health symptoms did not receive mental health treatment due to high cost and lack of access to the service [47]. In addition, the burden of these conditions disproportionately affect populations with limited access to mental health treatment [17]. In response to the rising mental health needs, mental health supports were embedded into mobile applications (apps) that provide supported care, illness management, symptom tracking, as well as teletherapy as a more convenient, accessible, and low-cost mental health care mechanism for people in need [6].

As the usage of mental health apps (MHA) increases [12], there is growing attention on the protection of user privacy in MHAs due to the sensitive nature of mental health data compared to other forms of health data [8] as well as the lack of regulatory oversight [21, 40]. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) [3] protects a consumer's health information collected by covered entities (e.g., health care providers, health plans, health care clearinghouses) from being disclosed to any parties without the consumer's consent. However, online therapy apps that are subjected to following HIPAA requirements, such as BetterHelp and Cerebral, sometimes fail to comply with these requirements by sharing users' personal information to third parties without users' consent [22, 72]. Outside of online therapy apps, MHA development companies, such as those that create self-management apps where users input their own data within the app, are not considered covered entities, so they are not required to comply with HIPAA regulations [2]. Some states have attempted to remedy this by requiring MHAs to provide more comprehensive privacy policies. For example, the California Consumer Privacy Act (CCPA) [1] requires privacy practices to be disclosed to users for apps that collect personal data. Yet, the privacy practice disclosures for MHAs are often unclear [31, 48, 60], inaccessible [34] and, even more egregiously, have been shown to be misleading [45].

Privacy risks associated with stigmas surrounding mental illness could have negative impacts on individuals' well-being [11, 46]. As such, for people who are vulnerable to harms due to their mental health conditions and need to seek mental health support, it is crucial to prioritize and protect their privacy when they engage in online mental health care. Moreover, vulnerable populations are more susceptible to violations of their privacy [63]. Prior work in the field of HCI has advocated for a more inclusive privacy and security design for under-studied populations [42, 77], including people with disabilities [28], older adults [43, 58], and people with visual impairments [67]. Yet, there is still a need for a more comprehensive

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

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642705

understanding on the data privacy and security concerns from actual MHA users to inform future privacy and security designs for people with mental health concerns.

In this paper, we aim to understand users' concerns regarding the data privacy and security of MHAs and compare them with concerns from privacy and security experts as well as mental health experts. We first qualitatively analyzed 437 user reviews pertaining to privacy and security of 83 apps from the U.S. Apple App and Google Play Stores to determine what data privacy and security aspects users are currently concerned with. We then compared these concerns with the concerns listed on two prominent app evaluation websites created and maintained by experts: Privacy Not Included and One Mind PsyberGuide. Our findings elucidate the gaps users have in understanding the potential risks of MHAs. However, we also identify a number of specific concerns that are not addressed by current assessment sites. We make recommendations for how MHAs can be better designed with privacy and security in mind, as well as how mental health practitioners can support their client's decision-making when choosing a MHA.

2 RELATED WORK

2.1 Privacy and Security Risks and Concerns for People Suffering from Mental Illnesses

Data privacy is becoming an important ethical consideration for mental health technologies as mental health data is regarded as more sensitive than other forms of health data [8]. The negative impacts on people's well-being due to stigmas surrounding mental illnesses can lead to social isolation, employment risks, negative therapeutic outcomes, aversion to treatment seeking, and more [18, 19, 27, 38, 44, 62]. Several studies have delved into the risks associated with the loss of privacy for people with mental health concerns when they engage in online activities [43, 46]. For instance, a study from Naslund and Aschbrenner highlighted that privacy risks for users with serious mental illnesses engaged in social media could lead to concerns about stigma and judgment from others and cyberbullying [46]. Likewise, other studies that explored online safety and privacy for autistic youths found that there are increasing privacy risks online that resulted in poorer well-being for those with autism compared to other non-autistic youth [41, 61]. However, to the best of our knowledge, the precise consequences of privacy violations on individuals suffering from mental illnesses remains unknown.

While research has demonstrated that MHAs can be effective interventions for alleviating symptoms of mental illness [23, 39], concerns about MHA user data privacy and safety have arisen among clinician and mental health practitioners [7, 21, 52, 69]. In a report published by the the American Psychological Association (APA) [21], psychologists urged other practitioners to use caution when recommending or implementing MHA in their practices. The report warns clinicians about the risk of data breaches and limits of data encryption, stating that, unlike information obtained and stored by the psychologist, data collected by MHAs are susceptible to outside forces such as hacking and interception, which limits a practitioner's ability to take the "reasonable precautions" of privacy and confidentiality as required by the APA ethics code [10]. There are also concerns about what a breach in data privacy could mean for the wellbeing of a patient [37]. The risk to a patient as well as the risk to ethical principles has led practitioners to be wary about the implementation of MHA in their practice [21, 40, 76].

Our work attempts to understand MHA users' concerns with mental health apps that collect, exchange, and store users' personal and health data. Past work in personal informatics and health (e.g. self-tracking [35, 74], mood tracking [64], intensive data monitoring [13, 14], health information exchange [66], mobile apps [20, 78]) have explored people's use and perspectives on data-driven support in mental health management. However, only a few studies specifically focused on the privacy perspectives of MHAs. In survey studies on people's perspectives on mental health data collection, researchers found that people are more willing to share health data than personal data as long as it is beneficial to their mental health [13, 20, 78]. On the other hand, Blair et al. and Shen et al.'s interview studies found that users' willingness to share health data are context-dependent and are based on the level of trust they have with the people they are sharing their data with [14, 66].

In this paper, we are interested in the experiences of users who engage with MHAs that collect users' data. By analyzing users' feedback on their experiences with MHAs, we are able to provide guidance to MHA users and experts from the fields of privacy and security and mental health technology to make informed decisions about the use of MHAs.

2.2 Data Privacy in MHAs

While it is important to ensure the safety and protection of data for users of MHAs, several studies found that the current MHA industry puts little effort into safeguarding users' data privacy and security while actively urging them to share information [32, 50, 51]. Furthermore, research has revealed that data sharing with third parties is a common practice in MHAs [31, 50], posing a potential threat to users' privacy. A recent study conducted by Iwaya et al. discovered that the data collected by MHA companies could be linked to users' identity, which could potentially result in the sharing of linkable data with the third parties [32].

However, users often have little or no way to be aware of such sharing practices when they engage with MHAs. While privacy policies are discoverable on MHA companies' websites, most policies require college-level reading comprehension abilities [32, 54, 60], and are not up-to-date [31] or transparent [48, 60] about their privacy practices. HCI researchers have explored methods to help users easily understand privacy policies using nutrition labels [36], comic strips [70], and interactive dashboards [59]. However, the privacy labels on popular app stores, such as the Apple App Store, are still difficult for users to decipher [79]. Moreover, Mozilla found that the privacy labels of apps on Google Play are often inconsistent with their privacy policies [45]. Without knowing how an app shares data, users could falsely assume that their data are kept private and secure within the app. This could result in companies profiting from vulnerable communities (i.e., people with mental health conditions) by exploiting this sensitive data.

To better understand MHA users' perspective on the data they share with the apps, we analyzed user reviews from 83 MHAs available on the Apple App and Google Play Stores. Previous work in HCI has conducted user review analysis on MHAs [15, 29] to

investigate users' experience and perspective and briefly mentioned privacy and transparency as part of their findings. To extend our understanding on MHA users' experience as well as their concerns regarding data sharing with MHAs, we conducted a two phase study. In Phase 1, we provide an in-depth analysis on user reviews related to data privacy. In Phase 2, we compared our findings to reports by experts given on Privacy Not Included and One Mind PsyberGuide.

2.3 Expert Evaluation Criteria

There are two expert evaluation sites that reviewed MHAs to provide guidance for people interested in using MHA — Privacy Not Included and One Mind PsyberGuide. On the former site, the apps were reviewed by privacy and security research experts [26], while on the latter, they were reviewed by mental health technology experts [57]. In this paper, we refer to these two sites as "experts."

2.3.1 Privacy Not Included. Mozilla's Privacy Not Included [24] buyer's guide has the aim to "help you navigate this landscape by understanding what questions you should ask and what answers you should expect before buying a connected tech product." For their analysis, they explain that they "look at things like privacy policies, company websites, news reports, research whitepapers, app store listings, consumer reviews, and anything else we can find and trust to inform our research" They do not purchase or download the app to evaluate it. They then assign a *Privacy Not Included Warning Label to those products if it receives two or more warnings from their criteria; this also means that each criteria is weighted equally. The criteria for assigning a warning listed on their website include: Permissions (including tracking), Privacy (including use and control of one's data), and Minimum Security Standards (including encryption and privacy policies). In addition, the website lists untrustworthy artificial intelligence as a concern consumers should be cognizant of; however, at the time of our analysis, the experts do not use that criteria in their warning label assessment due to the limited availability of information available from the product companies.

2.3.2 One Mind PsyberGuide. One Mind PsyberGuide [56] was developed by a non-profit organization and brings together experts in mental health practice, technology, and digital mental health. Expert reviewers score mental health apps on three categories credibility (i.e., is the app likely to have a positive effect on mental health), user experience (e.g., how fun and easy is using the MHA), and transparency (i.e., is information on data collection, storage, and exchange readily available and understandable). We specifically focus on the criteria specified in the last category here. App privacy policies are rated as acceptable, questionable, or unacceptable based on whether sufficient information is provided.

3 PHASE 1: MHA USER REVIEW THEMATIC ANALYSIS

In the first phase of this study we sought to understand the perspectives of MHA users' data privacy and security concerns. In the following subsections, we outline the methodological approach used to collect and analyze our data followed by the thematic findings.

3.1 Phase 1 Methods

We used an interpretivist approach to understand MHA users' experiences and perspectives on the data privacy and security of mental health apps. We conducted a qualitative analysis of user reviews from publicly available mental health apps. HCI researchers have employed user review analysis as a promising method to understand real-world users' experiences on mobile apps [15, 29, 30, 33]. Guided by past work that studied user review analysis of mental health apps [9, 15, 65, 68], we leveraged publicly available data from U.S. app stores to gather qualitative feedback from MHA users as well as from different types of mental health apps (i.e., self-care, teletherapy, peer support). While we did not identify users' demographics, nor did they leave identifying information in their reviews, we were able to collect user reviews from a wide range of individuals using apps designed for people with mental illness. The study is approved by our university's Institutional Review Board.

3.1.1 Selection of Sample Apps. We followed the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) four-phase process to ensure transparency in our data inclusion (see Figure 1) [49]. We identified apps from keyword searches and top free and paid "Health and Fitness" charts on Apple App store and Google Play from June to July 2023. We utilized "AND" and "OR" commands of "mental health", "therapy", and "care" when we performed the keyword searches on both app stores. In addition to browsing apps on both app stores, we used Google advanced search to find apps that did not show up on app stores due to the ranking algorithms. We applied the following inclusion and exclusion criteria:

- Inclusion criteria: (1) teletherapy, self-care, and peer support apps that specifically mentioned the type of care (e.g. guided meditation) or therapy (e.g. CBT), (2) apps that target mental health condition (e.g. anxiety, depression, addiction), and (3) apps available in English.
- Exclusion criteria: apps that (1) have less than 50 reviews, (2) were last updated prior to 2020, (3) do not collect data, (4) not available in English, (5) do not explicitly state targeting mental health conditions, and (6) do not explicitly state the type of care or therapy provided.

The first author carefully screened the descriptions of every app that appeared in the app store keyword searches, top "Health and Fitness" charts, and Google advanced search, and added those that met the inclusion criteria to the corpus (Apple App Store: n = 270, Google Play: n = 201). For each identified app, the first author retrieved the number of user reviews, the date of the latest version, and collected data from the privacy labels on the app stores. We aimed to focus on apps with high and active user engagement, and thus we decided to exclude apps that have less than 50 reviews and were last updated prior to 2020. Since privacy labels on popular app stores might be incorrect, as found by Mozilla [45], for apps that do not indicate any data collection on the app stores, the first author went to the app companies' websites to investigate whether there is a privacy policy. Additionally, the first author reviewed the app description and user reviews showing up on the app store's website to determine if there were any features that collected user data. Only after this thorough evaluation was a determination made as

to whether an app did not collect data and thus was not part of our evaluation. The exclusionary criteria were then applied, resulting in 140 discrete apps (Apple App Store: n = 87, Google Play: n = 94, with an overlap of 41 apps) that were included in the analysis (see Figure 1). We reported the final list of MHAs from both app stores in Appendix A.1 Table 1–3.

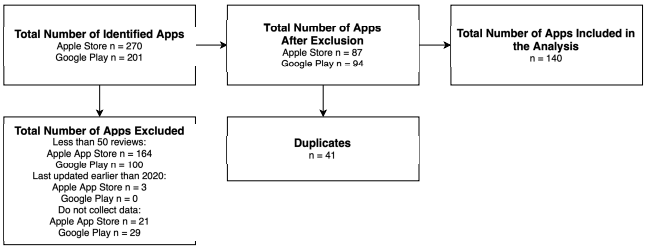


Figure 1: Flowchart of the Sampling Process for User Review Analysis

3.1.2 Data Collection and Analysis. We used an Apple App Store and Google Play scraper in Python to extract the latest 1000 reviews that were posted after 2020 of the included apps [4, 5]. We then excluded reviews that (1) were not in English, and (2) were fewer than 100 characters (according to previous study [75], the average length of the app user review is 117 characters). We applied our exclusionary criteria to ensure that the reviews we analyzed would generate meaningful insights. For apps that appeared on both the Google Play and Apple App Stores, we included user reviews from both platforms with an intention to include both android (Google Play) and iOS (Apple App Store) users in our analysis. This resulted in 23,968 reviews from Google Play and 31,120 reviews from Apple App Store.

Similar to the previous work [9, 15, 29, 68], we conducted a thematic analysis where we followed Clarke and Braun's [16] six stages of thematic analysis. However, given our study's specific focus on privacy and security concerns, we included only reviews relevant to the study's scope. This approach was well-suited to identify a wide range of privacy and security concerns raised by users.

The first two authors familiarized themselves with the data by screening randomly selected reviews. Then, we defined reviews as "relevant" and "irrelevant" based on users' experience with data and perspectives on privacy and security. Specifically, reviews that are relevant to the scope of this study are those that reflecting users' experiences with sharing data with the apps. This includes personal information (e.g., name, email address, credit card number, biometric data), mobile sensing data (e.g., audio recordings, location data), and health data (e.g., tracked physical or mental data, mood journal entries, PHI). Examples of "irrelevant" are those pertaining to app usability issues, cost concerns, or reviews that only mention a feature without explaining the user experience.

The first two authors and an undergraduate research assistant screened the reviews together from randomly apps based on the definition of "relevant" reviews to discuss any uncertainty about what constitutes "relevant" and "irrelevant" until a consensus was reached. Then, all three researchers independently screened all reviews collected from each app store and kept each other informed of any uncertain reviews in order to reach a consensus on them. The process of narrowing down the reviews as shown in Figure 2.

The first two authors then assigned initial codes to the identified user reviews using an inductive approach. After gathering the codes into candidate themes, all authors reviewed the themes together and conceptualized new themes and subthemes. At the end of the analytic process, we had identified 437 reviews from 83 discrete apps that were relevant to the scope of the study, with a total word count of 36,759 for all reviews and an average of 84 words per review. We then organized them into four themes: types of data being collected, third party involvement, data safety, and agency. Final set of inductive codes are available in Appendix A.1 Table 4. We report themes as subsections in Findings. Since the user reviews contain sensitive information, we paraphrased the quotes presented in the following section, as it is the best practice to reduce the risk of user profiles being identified [73].

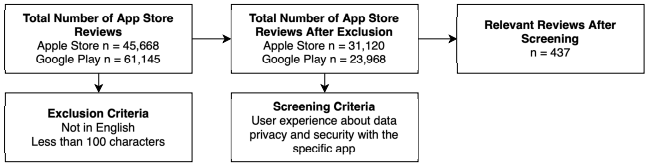


Figure 2: Process of Narrowing Down the User Reviews Relevant to the Study

3.2 Phase 1 Findings

3.2.1 Types of Data Being Collected. Our first reported theme demonstrates that users are concerned when asked to provide data linked to their identity. This includes personal information including first and last name, date of birth, phone number, email address, as well as biometric identifiers including fingerprints and facial recognition. Users often referred to the collection of identifying information as *"intrusive"* and *"unnecessary"*. A number of reviews also expressed concerns when the app requested protected health information (PHI) governed by HIPAA regulations. For instance, in comment R306, the user stated that they were *"not comfortable with non-professionals to collect my HIPPA information."* This comment and ones similar to it highlight that users are hesitant when asked for identifying information by an app which they may not fully trust because they understand the potential risks associated with providing that information.

Users expressed similar concerns about granting permission to track data on their devices, indicating that they were uncomfortable when the app tracks their browsing history and purchase history:

> *"The amount of personal data that it collects is crazy! I get that they might collect certain data to make things run smoother. Why is it necessary to monitor my personal browsing history or purchases? Why do they need to gather so much of my personal information? You can't even use all the features without agree to their data collection practice." (R41)*

On the other hand, some users held negative views toward what they referred to as *"anti-privacy"* trackers collecting personal and

device information, as indicated by this comment from R419: *"Decent app, but has anti-privacy trackers. I'm willing to invest for such an app, but not if it uses trackers from Google and Facebook."* Even though users may initially find the app helpful, their opinions shift negatively once they become aware of the presence of trackers that potentially invade their privacy.

3.2.2 Third Party Involvement. The theme of third party involved arose from reviews indicating users' concerns regarding data sharing or selling to other platforms for advertising purposes. User comment R263 expressed the user's concerns in an ironic manner, stating, *"Expecting to receive spam emails from people who has my medical information once it's sold to the highest bidder. Shady."* This user seemed particularly worried about the potential, undesirable consequences of data selling - receiving spam emails. Another user had also received emails from third party services and wrote, *"They may claim they don't sell your information, but I've begun to receive emails from other mental health services. Coincidence? Definitely not." (R101)* This user noticed that their data might have been shared to third party advertisement companies based on the unusual emails they received. Unlike previous quote, however, this quote suggested that the user lost their trust of the app after they began receiving spam emails from marketers.

Apart from data sharing for advertising purposes, some users identified other third parties that might collect their data for non-advertising purposes, with whom they would prefer not to share their data. For instance:

> *"Your policies provide ample room to change your mind. My personal, sensitive data about my well-being might be sold if your company is sold out or declares bankruptcy. What if my health insurance provider or my employer gets it?" (R31)*

After reading the MHA company's policy, this user was particularly concerned about how their data could be sold to health insurance companies or accessed by employers. Such scenarios could potentially impact their insurance rates as well as employment status. Findings in this theme highlight user uncertainty and distrust regarding how the MHA companies utilize their sensitive data.

3.2.3 Data Safety: Mishandling data. Some reviews mentioned undesirable outcomes that made users suspicious about how the app mishandled their confidential data, specifically regarding the usage of data without users' consent. For example in an online therapy app, one user mentioned that their therapist abused the information that was shared:

> *"The therapist assigned to me abused my trust. They asked me to recommend solutions to another patient where they revealed the patient's name and personal information, violating patient's confidentiality. I felt disregarded, manipulated, and as if I was paying to be exploited. This violates my trust and harms my mental health." (R27)*

It was evident that the therapist on this platform violated HIPAA regulations by disclosing another patient's personal information. This comment is particularly alarming when considering that therapists are trained to adhere to HIPAA regulations not only for legal reasons, but also to uphold the ethical principles and expectations of therapists [10]. In addition to triggering negative emotional states in users, mishandling of data can also lead to security risks in other, not mental health related apps. For example, this user became suspicious about the data that they provided to the mental health app they used when encountered a potential security breach on their personal Google account:

> *"They request for an email and password when installing and opening the app makes me kind of suspicious. What's even more concerning is receiving a notification about an attempted login to my Google account. It could have been a coincidence, but the occurrence of both events together suggests that the creators might be accessing, hacking, or otherwise obtaining people's emails due to having access to their passwords."*

While the collection of identifying data itself raised concerns, the attempted, unauthorized access to the user's personal Google account raises even more concern. Unfortunately, this review also indicated that, although the user may have been aware that sharing personal information carries risks, this awareness did not deter them from providing said personal information. It was only when the risks were realized that they started to become genuinely concerned about their online security. Fortunately, from the user review, it appeared as though the user intervened before their Google account had been accessed.

Other reviews also demonstrated user awareness and alertness about their data safety, consuming online information (i.e., Federal Trade Commission reports, Privacy Not Included) to assess the security of the specific app they were using. For instance, one user of the Cerebral app, an app that has been subject to intense public scrutiny, left a review stating: *"They recently had a breach that leaked every patient's data, even their social security number. So that's GREAT." (R96)* In this review, the user indicated that they not longer trusted this company due to their concerns about how the app misused others' personal information.

According to news reports, Cerebral shared 3.1 million users' personal information through tracking technologies from third parties without users' consent [72]. Among that information were PHI, information that, under HIPAA, are expected to be kept confidential. Reviews of other apps also indicate the sharing of PHI and other personal information, and news stories continue to report of data breaches within MHAs. As a result, users lose trust in MHAs as concerns for their own safety increase.

3.2.4 Data Safety: Lacking security measures. Among users who expressed concerns about the lack of security measures, many emphasized the importance of security settings, such as password, passcode, or face ID to prevent others with access to their phones from accessing their diary entries in the app. In R184, this user suggested a security lock to ensure the privacy of their data: *"I suggest to add an optional security lock feature. I wouldn't feel comfortable if anyone else could open this and see everything since it's private."* Users value their privacy and want assurance that the people around them will not be able to access their mental health data entries. Therefore, a security setting that prevents others from accessing the app appears to be an essential feature when users engage with MHA that stores users' diary entries as well as other forms of health information.

Other reviews mentioned the lack of encryption of the data. Without a clear assurance of data encryption, users are unwilling to provide their personal information due to concerns about unauthorized access to their data. For example in R153, the user wondered:

> *"Where's the end-to-end encryption? It would be very helpful and reassuring if app's contents are encrypted because people are storing the history of their life on this app. Without this type of encryption, the entries are visible to anyone else with access to Apple's servers."*

This user seemed very much aware of the risks of storing unencrypted information on the MHA's server. The lack of transparency regarding how their data were being protected within the app led to the user questioning the safety of their data.

Finally, concerns regarding the lack of protection for vulnerabilities, specifically minors and individuals with mental illnesses, were raised on multiple occasions. Concerns related to minors were mostly brought up in apps where users interacted with other user-generated content (e.g., peer support) and AI-generated response (e.g., chatbot). In R57, the user mentioned: *"They failed to implement any measure to protect minors from accessing the app, and they collected their data. It's as if their legal team is a bunch of drunks."* Here, the user expressed worry that the app failed to consider the protection of minors in the data collection process. This user also indicated that such an occurrence may be an illegal act. A number of other reviews mentioned that the app not only failed to protect vulnerable users, but also exploited the vulnerabilities of individuals with mental illness to collect personal information for potentially nefarious reasons. For instance, this review clearly indicated users' concerns about the private information that was gathered during the process of addressing cognitive distortion:

> *"People use this app to sort through their most private and personal thoughts and feelings. The app developers are responsible for protecting the private information they collect, especially considering its therapeutic nature. These developers target vulnerable people, encouraging them to share their private thoughts in the app to seek help. They exploit data obtained from individuals who are uninsured and under-insured to line their own pockets. Apps like these need more federal oversight." (R142)*

While individuals with mental health conditions are in need of the support to alleviate their condition, this user was particularly concerned that the app exploited this "need" to collect private information. Moreover, this user explained that the app developer had a responsibility to protect such information but, instead, used the information to profit off vulnerable users.

3.2.5 Agency: Ownership of the data. Users demonstrated concern about the lack of control over their data. Specifically, they were worried about not being able to manage their data after it had been collected. This included the inability to edit and delete personal information and other data entries from the MHA, an instance sometimes refer to as *"no respect for [their] privacy"*. When requesting to delete personal information, one user became suspicious when their request was not fulfilled: *"They won't remove your information. It'll remain in their system for years, ready to be sold. They charged my credit card and refused to remove my personal data." (R101)* Not being able to remove personal information upon request elevates users' concerns that the company will share their information with third parties without their consent. Similarly, when considering the risks associated with collection of personal information, users are worried about not being able to control data sharing with third parties.

> *"The app may claim to be free, it actually sell your data without a way to opt out of it with 'do not sell my data' feature. This is concerning because paying a small subscription fee cost far less than having your mental health information sold to third parties. Basically, their privacy policy is very weak." (R214)*

As demonstrated in the above review, the user wondered why it was not possible to avoid sharing their data with third parties and suggested that they would prefer to pay the MHA developer than risk their privacy being violated by the developer selling their data for a profit. A willingness to pay for data protection and ill-reactions to not being able to manage their data shows how concerned users are that, once they provide their information, they will lose the ownership of their personal data. In other words, the company remains in full control over a users' data.

3.2.6 Agency: Manipulative data practices. When asked to provide personal information, many users reported concerns about deceptive data collection practices. Specifically, apps *"forces"* users to input personal information to proceed with using the app without giving the option to skip through the data collection process. Several reviews mentioned that an app compelled users to give permission to receive emails and did not offer an option to opt out, as seen in this review: *"They force you to enter your email to see your results and do not provide an option to unsubscribe from future emails. I'll probably end up on every freaking spam list out there." (R131)* This user indicated that the app employed a deceptive strategy to entice users to provide their email addresses to access app content while denying them the choice to opt out of the email list. Under such manipulative practices, users are more likely to provide information against their will in exchange for access to personalized app content.

In addition, users are concerned about the lack of transparency regarding data practices, even when they read the privacy policy. Without complete disclosure from the app, users often remain uninformed about the usage of their personal data. In one review, a user wrote R178 state:

> *"They did not disclose whether your information is used for marketing purposes. For example, if you are trying to improve your fitness, you will start receiving with ads for gyms and personal trainers. Even after reading their privacy policy, it's still not clear."*

This example illustrates that the user perceived no way to find detailed information about the data sharing practices from publicly available content. Moreover, some reviews also mentioned the inability to contact the company regarding the privacy policy, as seen in this review: *"I contacted the email address listed in their privacy policy because I have questions about it, but it came up as undeliverable." (R186)* Even when the user proactively sought out more clarity on the privacy policy, they were met with roadblocks

that prevented them from getting answers, perpetuating the loss of agency over their own data once provided to the app.

Lastly, users consistently brought up the unethical data usage from the app. Many users complained about unauthorized charges to their credit cards, the inability to cancel app subscriptions, and other, unexpected charges after providing payment information. Oftentimes, apps allow users to access the app using a *"free trial"* while charging immediately after they signed up. As seen in this review: *"When I signed up and tried the free trial, they immeidately charged my card. That's just sketchy to me." (R80)* In this case, the app deceived users by claiming there was a *"free trial"* in order to access the user's payment information. Even more, many users indicated that an app will *"randomly charge"* them without their consent.

> *"They'll store your card details and randomly charge you after you've canceled your subscription. My wife canceled before the free trial ended but still got charged. We canceled a year ago but still got charged today." (R176)*

From this review, it becomes evident that once the user provides their payment information, an app will charge the user at its own discretion, leaving the user without any control over their finances. Several reviews also revealed how apps will employ a paywall to block users' access to their data until a payment is received, as this review stated: *"I'm sure it's against the law to restrict access to users' private medical data behind a paywall. So disappointed." (R389)* In this and similar instances, the app, essentially, held a user's data hostage, demanding money before allowing a user access to their own, private data. The lack of regulations surrounding the actions of MHAs may be a contributing factor to this happening as many app companies appear to prioritize profit over user data privacy and security.

4 PHASE 2: COMPARISON OF MHA USERS' PRIVACY AND SECURITY CONCERNS TO THOSE IDENTIFIED BY EXPERTS

In the second phase of this study we collected the privacy and security concerns from two prominent app review websites and then compared those concerns to the concerns identified in Phase 1 of the study.

4.1 Comparison of User to Expert Concerns

There are two prominent app evaluation websites that provide information to concerned users who are evaluating the privacy and security of a MHA: Privacy Not Included and One Mind PsyberGuide. We collected evaluation criteria listed on both websites [25, 55], referred to as "expert concerns", and compared them with the concerns from the user review. The expert concerns are listed on the right side in Figure 4.

Figure 3 presents the process of how we analyze the user review data and compare it with experts' concerns. From Phase 1, we had 60 low-level codes (see Appendix A.1 Table 4) to compare to expert concerns collected from the websites. Many of these codes overlapped in concept and were only different in specific application (e.g. data selling to marketers, data sharing with third parties). We combined these codes, referred them as "MHA user concerns", and correlated them to the expert concerns that have the similar meaning, as shown in Figure 4. After this mapping exercise, we were left with user app review codes that were not addressed by any of the expert websites. Finally, we counted how often each user app review code was used and transferred that as a percentage of the total number of concerns coded. In the following section we present the comparison between the codes and the percentage of occurrence as a heat map and then discuss those differences.

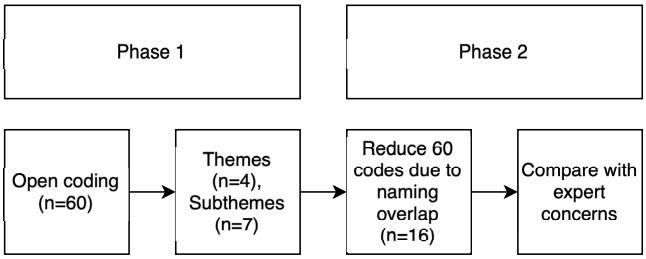


Figure 3: Process of Comparing 60 Open Codes to Expert's Concerns

.

4.2 Phase 2 Findings

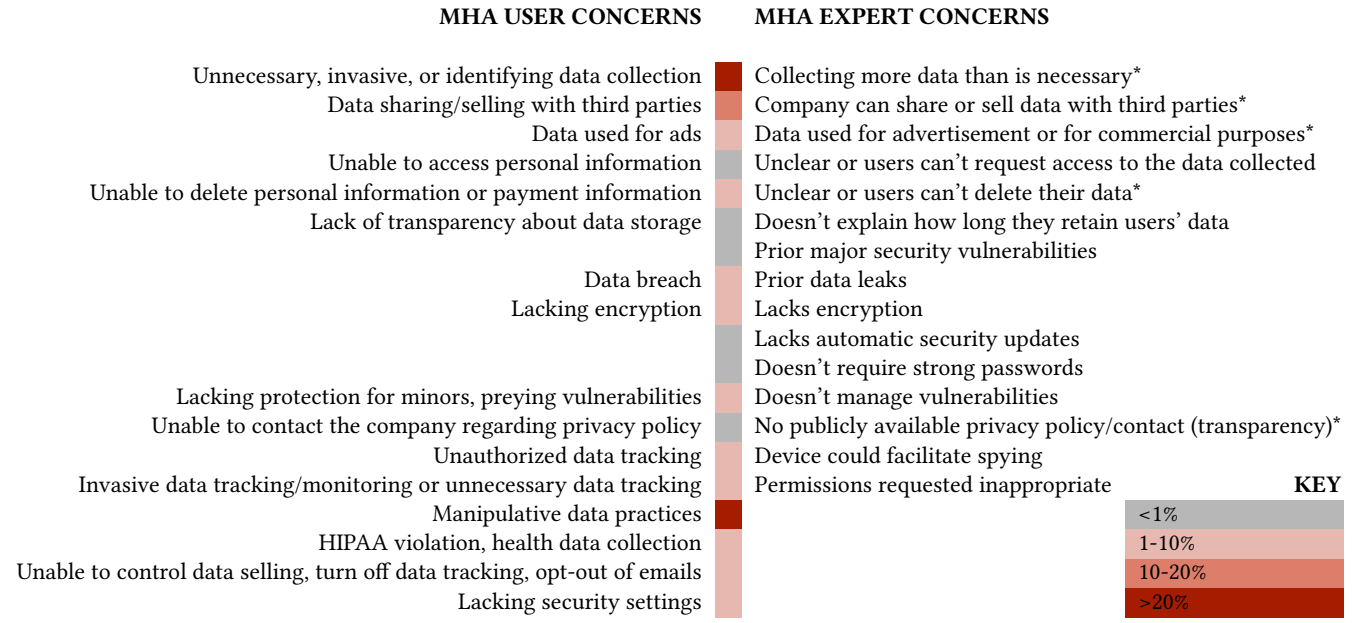
Figure 4 lists the combined concerns from these two websites and compares them to the concerns we have outlined in our Findings. We have presented the findings as a Heat Map showing the relative frequency of each user concern that arose in our data analysis.

In the following subsections we discuss how the concerns outlined on these two expert app evaluation websites compare to our users' concerns. When comparing themes and subthemes to the categories of evaluation criteria established by Privacy Not Included and One Mind PsyberGuide, we found that a portion of users' concerns aligned with most of the expert criteria. However, there was still a mismatch between users' and experts' concerns regarding user data privacy and security.

4.2.1 Where user concerns aligned with the expert criteria. Many users mentioned privacy concerns related to the collection of their identifying information and expressed worries that the app might share or sell their data to third parties without their consent. Furthermore, users raised concerns about their inability to edit and delete their personal information, indicating a lack of control over their data. Both of these issues align with the privacy expert criteria outlined by Privacy Not Included. In addition to the privacy evaluation criteria, data tracking also emerged as a significant concern among users, particularly with regard to permission requests that were perceived as intrusive and unnecessary. When it came to security measures, a few users touched on the lacking encryption and lacking protection for vulnerable populations (e.g., minors, people with mental illness), as well as an app's prior record of data breach. This also matched the expert criteria.

4.2.2 Where users did not mention expert criteria. Even though our user reviews covered a significant portion of the categories in the evaluation criteria, there were six expert criteria that were not mentioned or were only mentioned once or twice in the user

Table 1: Heat Map of User and Practitioner Concerns Compared to Expert Evaluator Concerns (* indicates those by both Privacy Not Included and One Mind PsyberGuide)



reviews. Three of these fall into the "minimum security standard" category, specifically concerning the lack of automatic security updates, lack of a requirement for strong passwords, lack of a publicly available privacy policy, and lack of contact. Among all the user reviews included in this study, no reviews mentioned lack of automatic security updates or requirements of strong passwords, and only two mentioned an inability to contact the MHA development company. The lack of user reviews about these evaluation criteria may suggest that users are not as concerned as experts with those aspects of MHAs.

4.2.3 Where users had concerns that were not being evaluated by experts. When it comes to the data collection process, users specifically mentioned concerns about the confidentiality of their PHI and potential HIPAA violations by the app. However, it is unclear how well users understand what information is protected under HIPAA solely by mentioning its violation in their reviews. Nevertheless, users mentioned HIPAA violations on multiple occasions, but experts failed to include the following of HIPAA guidelines as an evaluation criteria on their websites.

The expert criteria also falls short in offering a comprehensive review of the control users should have over their data. Some users noted that they were unable to disable data tracking, data sharing, and opt out of email lists after providing their personal information. However, the expert criteria only covered a user's ability to request and delete their data. Additionally, users highly value their privacy, especially regarding control over data access by others. From user reviews, we observed concerns about the lack of security settings (e.g., data password or passcode protection) for controlling access. Both experts did not include this aspect as a criterion.

Lastly, neither of the experts addressed user experience aspects that contribute to users' concerns about data privacy and security. Users mentioned manipulative data practices by MHAs that unethically and deceptively collect users' data, causing emotional and, sometimes, monetary distress. Additionally, some users expressed concerns about companies not adhering to their privacy policies, which also was not included in the criteria on both expert websites.

5 DISCUSSION

This study analyzed 437 reviews from 83 MHAs from Apple App and Google Play Stores within the scope of privacy and security concerns. We distinguished our study from prior research that explores users' perspectives and experiences with MHAs [15, 29] as well as people's attitudes towards data-driven mental health management on smartphone apps [20, 78] by investigating actual users' experience with data sharing in MHAs. Furthermore, we juxtaposed those user experiences with expert criteria to compare and contrast what the experts believe users should be aware and concerned of in terms of data privacy and security and what users are actually aware and concerned of. Despite previous studies that found that users are willing to share their data to receive valuable health feedback in different contexts [13, 14], our findings indicate that there is still a portion of users who have a myriad of concerns when asked to provide their personal information.

Our findings also suggest that even though people who are concerned about their privacy and security are acutely aware of the collection of identifying information by MHAs and have a similar

understanding of the implications of their data being collected by MHAs as mental healthcare providers [9], they do not seem to fully understand the potential dangers they face. In the context other than of MHAs, a study by Tabassum et al. on end-user perception of data practices in smart homes also shows that users are not fully aware of the potential misuse of their data [71]. On the other hand, a study by Rocheleau and Chiasson on the perspectives of autistic teenagers regarding privacy and safety on social networking sites found that these teenagers are aware of their privacy and safety, prompting them to adopt different approaches to protect themselves online [61]. This suggests that individuals who are vulnerable, such as autistic teenagers who are more susceptible to privacy and safety risks, might be more conscientious about protecting themselves online. However, data from user reviews suggests that although users are aware of data collection, they are not deterred from providing information to the app. It is only when undesirable outcomes actually occur that users become cognizant of the risks associated with data collection. Unfortunately, understanding these risks after data has been shared may be too late as the information is typically stored on company servers where users may have limited control over it. Furthermore, even when individuals proactively seek clarification on data privacy practices, MHA companies often failed to provide full disclosures in their privacy policy, which is consistent with prior work's finding on the lack of transparency in privacy policies [48, 60].

Our study contributes to not only understanding users' privacy and security concerns, but also how users' concerns differentiate from experts' concerns that were incorporated into app experts. Our findings have important implications for MHA users to make informed decisions when choosing the app and mental healthcare practitioners that may be recommending such apps to their clients, as well as for those app experts who are trying to provide guidance to MHA users.

5.1 Implications for Better MHA User Guidance and Education

As highlighted in Phase 2 of this study, there are publicly available expert resources such as Privacy Not Included and One Mind PsyberGuide to help guide users when assessing the privacy and security of a MHA. However, the former only includes a small subset of the available mental health apps and the latter does not dive as deeply into privacy and security. This means that there is still a large gap in the resources available to support both MHA users and mental healthcare providers in their decision making around MHAs. In addition to better, widespread MHA users and mental healthcare professional education, a more robust online resource is needed.

The experts behind Mozilla's Privacy Not Included and One Mind PsyberGuide have clearly put in significant effort to review, at a minimum, dense, convoluted privacy policies. In fact, Privacy Not Included goes beyond that, seeking out additional publicly available online resources, such as records of data breaches, to include in their reports on the website. However, our analysis on the comparison of user concerns derived from user reviews and expert concerns presented in two app evaluation websites suggests that user concerns present opportunities for experts to consider in their app evaluation: adding explicit HIPAA evaluation criteria for mental health apps, weighting criteria, and incorporating the user voice in evaluations.

Despite the comments invoking HIPAA, it remains unclear to us whether MHA users have an accurate understanding of what this policy entails. In this area, experts can help clarify HIPAA regulations by adding further criteria related to HIPAA in their assessment of MHAs. Specifically, this could involve identifying whether or not the apps are considered covered entities, determining whether PHI is collected, and evaluating whether the apps adhere to HIPAA regulations if they are indeed covered entities.

However, both Privacy Not Included and One Mind PsyberGuide specifically state that they do not test the apps. Given that our analysis suggests that there are user concerns that are not currently being evaluated on these websites, including user reviews or another sources that brings in the voice of the user to better understand actual in-app experiences could be critical to fully capture the range of relevant privacy and security concerns. Privacy Not Included attempts to mitigate this disconnect by including a 'Creep-O-Meter' where consumers can read about an app (or other product) and rate its level of creepiness. However, the person rating does not necessarily need to be a user, and this is a rigid measure that does not allow individuals to explain what exactly they find creepy.

Monitoring user reviews on app stores for privacy and security concerns may currently be the best option for large-scale understanding of user privacy and security concerns. User experiences with MHA may be unique to the individual, but those experiences can still provide valuable input and insight that other, potential users may benefit from. It might also be helpful for users if they assigned a weight to the various criteria being assess on these websites while also customizing their Creep-O-Meter report.

5.2 Limitations

Our findings are based on the analysis of user reviews from MHAs in the Apple App Store and Google Play. One limitation of gathering data from these platforms is that there is no way to determine whether the reviews are fake. As we analyzed the user reviews, we attempted to identify fake reviews and excluded them from the analysis by observing the timing patterns, recurring phrases across different reviews, and the distribution of star ratings. Furthermore, the scope of the study is centered on users' experiences and perspectives related to data privacy and security, which led to the exclusion of reviews that were too generic and did not provide meaningful insights into user experiences and concerns related to data privacy and security. However, even though we excluded a number of reviews that were irrelevant to the scope of this study, we were able to conduct an in-depth qualitative analysis of all the relevant reviews related to privacy and security concerns from a significant number of MHAs (n = 83) available on the market.

Another limitation of analyzing user reviews is that we might overlook input from users who do not express their privacy and security concerns through app reviews. Furthermore, unlike other qualitative methods such as interviews, this method does not allow further probing with users to uncover a deeper understanding of their concerns. However, we have identified 60 lower-level codes

as users' concerns relevant to privacy and security from a large sample of MHAs and users. This provides a good starting point to understand users' concerns from a large-scale perspectives for future work that could employ other methods, such as interviews or surveys, to further explore users' concerns related to privacy and security in MHAs.

5.3 Future Work

There is a discrepancy between experts' evaluations and users' concerns for several apps. While the experts may not be identifying any privacy and security issues based on what is stated in the privacy policy, users have raised concerns in their reviews. It is unclear whether it is the app that does not follow its privacy policy or if users have misunderstood the situation. More research is needed to disentangle policy, end-user license agreement (EULA), practice, and perceptions as well as justify if users' concerns are valid for the specific app.

Furthermore, understanding what MHA users might do when provided with guidance that includes a comprehensive list of users' privacy and security concerns would contribute to our knowledge of how we can better support their decision-making process. Such information could lend itself to being the start of a series of educational materials aimed to help users understand data privacy and security, how to evaluate an app's safety and privacy policies, and how to better protect themselves from data breaches due to deceptive in-app practices.

Finally, the comparative findings suggest that the guidance provided to users for making informed decisions on choosing an MHA may not be sufficient. Therefore, future research could explore other forms of guidance, such as input from mental health providers. It would be worthwhile to investigate what mental health providers are aware of when they recommend apps to their clients.

6 CONCLUSION

As the MHA market continues to grow [12] and more apps proliferate app stores, the risk of data privacy and security breaches may increase without intervention from regulatory bodies that protect patients and MHA users such as the Federal Drug Administration (FDA), Federal Trade Commission (FTC), and Office for Civil Rights (OCR). Researchers have demonstrated the ill-effects as a result of stigma on people when their mental health data are exposed, underlying the importance of maintaining user data privacy and security in regards to data stored on MHAs [11, 18, 19, 27, 38, 43, 44, 46, 62]. Our research further underscores this importance by providing insights from real users about the challenges they are currently experiencing with MHAs resulting from data mishandling, lack of security measures, violations of data agency, third party involvement, and unclear data collection policies.

While there exists resources created by experts to assess the privacy and security of MHAs, our results also indicate that there is a disconnect between what those security experts warn against and what users are experiencing in real-life. Users and practitioners alike should remain aware of both the consequences of data privacy violations and how to select secure and safe MHAs for use.

For the foreseeable future, it appears that the popularity and development of MHAs will not dissipate. In order to ensure user safety, the security of data collection and handling processes within MHAs must be held to a higher standard. MHAs have the potential to make mental health care more accessible to all peoples [7], but the move towards accessible mental health care should not come at the risk of user privacy and security.

ACKNOWLEDGMENTS

We thank Danielle Anane for assisting us in screening user reviews.

REFERENCES

[1] 2016. California Consumer Privacy Act (CCPA). Retrieved September 13, 2023 from https://oag.ca.gov/privacy/ccpa
[2] 2016. Health App Use Scenarios & HIPAA. Retrieved September 13, 2023 from https://www.hhs.gov/sites/default/files/ocr-health-app-developer-scenarios-2-2016.pdf
[3] 2022. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Retrieved September 13, 2023 from https://www.cdc.gov/phlp/publications/topic/hipaa.html
[4] 2023. app-store-scraper 0.3.5. Retrieved September 13, 2023 from https://pypi.org/project/app-store-scraper/
[5] 2023. google-play-scraper 1.2.4. Retrieved September 13, 2023 from https://pypi.org/project/google-play-scraper/
[6] 2023. Technology and the Future of Mental Health Treatment. Retrieved September 13, 2023 from https://www.nimh.nih.gov/health/topics/technology-and-the-future-of-mental-health-treatment
[7] Adrian Aguilera. 2015. Digital technology and mental health interventions: Opportunities and challenges. *Arbor* 191, 771 (2015), a210–a210.
[8] Mhairi Aitken, Jenna de St Jorre, Claudia Pagliari, Ruth Jepson, and Sarah Cunningham-Burley. 2016. Public responses to the sharing and linkage of health data for research purposes: a systematic review and thematic synthesis of qualitative studies. *BMC medical ethics* 17, 1 (2016), 1–24.
[9] Felwah Alqahtani and Rita Orji. 2020. Insights from user reviews to improve mental health apps. *Health informatics journal* 26, 3 (2020), 2042–2066.
[10] American Psychological Association. 2017. Ethical Principles of Psychologists and Code of Conduct. https://www.apa.org/ethics/code/ethics-code-2017.pdf
[11] American Psychiatric Association. 2020. Stigma, Prejudice and Discrimination Against People with Mental Illness. Retrieved September 13, 2023 from https://www.psychiatry.org/patients-families/stigma-and-discrimination
[12] Maryam Aziz, Aiman Erbad, Mohamed Basel Almourad, Majid Altuwairiqi, John McAlaney, and Raian Ali. 2022. Did Usage of Mental Health Apps Change during COVID-19? A Comparative Study Based on an Objective Recording of Usage Data and Demographics. *Life* 12, 8 (2022), 1266.
[13] Kitti Bessenyei, Banuchitra Suruliraj, Alexa Bagnell, Patrick McGrath, Lori Wozney, Anna Huguet, Bernice Simone Elger, Sandra Meier, and Rita Orji. 2021. Comfortability with the passive collection of smartphone data for monitoring of mental health: an online survey. *Computers in Human Behavior Reports* 4 (2021), 100134.
[14] Johnna Blair, Dahlia Mukherjee, Erika FH Saunders, and Saeed Abdullah. 2023. Knowing How Long a Storm Might Last Makes it Easier to Weather: Exploring Needs and Attitudes Toward a Data-driven and Preemptive Intervention System for Bipolar Disorder. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–12.
[15] Dionne Bowie-DaBreo, Corina Sas, Heather Iles-Smith, and Sandra Sünram-Lea. 2022. User perspectives and ethical experiences of apps for depression: A qualitative analysis of user reviews. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–24.
[16] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.
[17] Nicholas C Coombs, Wyatt E Meriwether, James Caringi, and Sophia R Newcomer. 2021. Barriers to healthcare access among US adults with mental health challenges: A population-based study. *SSM-population health* 15 (2021), 100847.
[18] Patrick W Corrigan, Benjamin G Druss, and Deborah A Perlick. 2014. The impact of mental illness stigma on seeking and participating in mental health care. *Psychological Science in the Public Interest* 15, 2 (2014), 37–70.
[19] Estefanía Del Rosal, Clara González-Sanguino, Sara Bestea, Jennifer Boyd, and Manuel Muñoz. 2021. Correlates and consequences of internalized stigma assessed through the Internalized Stigma of Mental Illness Scale for people living with mental illness: A scoping review and meta-analysis from 2010. *Stigma and Health* 6, 3 (2021), 324.
[20] Daniel Di Matteo, Alexa Fine, Kathryn Fotinos, Jonathan Rose, Martin Katzman, et al. 2018. Patient willingness to consent to mobile phone data collection for mental health apps: structured questionnaire. *JMIR mental health* 5, 3 (2018), e9539.

[21] Amanda Edwards-Stewart, Cynthia Alexander, Christina M Armstrong, Tim Hoyt, and William O'Donohue. 2019. Mobile applications for client use: Ethical and legal considerations. *Psychological Services* 16, 2 (2019), 281.

[22] Lesley Fair. 2023. FTC says online counseling service BetterHelp pushed people into handing over health information – and broke its privacy promises. Retrieved September 13, 2023 from https://www.ftc.gov/business-guidance/blog/2023/03/ftc-says-online-counseling-service-betterhelp-pushed-people-handing-over-health-information-broke

[23] Joseph Firth, John Torous, Jennifer Nicholas, Rebekah Carney, Abhishek Pratap, Simon Rosenbaum, and Jerome Sarris. 2017. The efficacy of smartphone-based mental health interventions for depressive symptoms: a meta-analysis of randomized controlled trials. *World Psychiatry* 16, 3 (2017), 287–298.

[24] Mozilla Foundation. 2023. Privacy Not Included - Mozilla Foundation. Retrieved November 27, 2023 from https://foundation.mozilla.org/en/privacynotincluded/

[25] Mozilla Foundation. 2024. About our Methodology *Privacy Not Included. Retrieved February 08, 2024 from https://foundation.mozilla.org/en/privacynotincluded/about/methodology/

[26] Mozilla Foundation. 2024. Why We Made This Guide *Privacy Not Included. Retrieved February 08, 2024 from https://foundation.mozilla.org/en/privacynotincluded/about/why/

[27] Faye A Gary. 2005. Stigma: Barrier to mental health care among ethnic minorities. *Issues in mental health nursing* 26, 10 (2005), 979–999.

[28] Foad Hamidi, Kellie Poneres, Aaron Massey, and Amy Hurst. 2018. Who should have access to my pointing data? privacy tradeoffs of adaptive assistive technologies. In *Proceedings of the 20th international acm sigaccess conference on computers and accessibility*. 203–216.

[29] Md Romael Haque and Sabirat Rubya. 2022. " For an app supposed to make its users feel better, it sure is a joke"-an analysis of user reviews of mobile mental health applications. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–29.

[30] Steffen Hedegaard and Jakob Grue Simonsen. 2013. Extracting usability and user experience information from online user reviews. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2089–2098.

[31] Kit Huckvale, John Torous, and Mark E Larsen. 2019. Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. *JAMA network open* 2, 4 (2019), e192542–e192542.

[32] Leonardo Horn Iwaya, M Ali Babar, Awais Rashid, and Chamila Wijayarathna. 2023. On the privacy of mental health apps: An empirical investigation and its implications for app development. *Empirical Software Engineering* 28, 1 (2023), 2.

[33] Jincheul Jang and Mun Yong Yi. 2017. Modeling user satisfaction from the extraction of user experience elements in online product reviews. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. 1718–1725.

[34] Sagar Jilka, Sara Simblett, Clarissa M Odoi, Janet van Bilsen, Ania Wieczorek, Sinan Erturk, Emma Wilson, Magano Mutepua, and Til Wykes. 2021. Terms and conditions apply: critical issues for readability and jargon in mental health depression apps. *Internet Interventions* 25 (2021), 100433.

[35] Christina Kelley, Bongshin Lee, and Lauren Wilcox. 2017. Self-tracking for mental wellness: understanding expert perspectives and student experiences. In *Proceedings of the 2017 CHI conference on human factors in computing systems*. 629–641.

[36] 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.

[37] Ido Kilovaty. 2021. Psychological data breach harms. *NCJL & Tech.* 23 (2021), 1.

[38] Robin Marie Kowalski, Megan Morgan, and Katlyn Taylor. 2017. Stigma of mental and physical illness and the use of mobile technology. *The Journal of Social Psychology* 157, 5 (2017), 602–610.

[39] Teghan Leech, Diana Dorstyn, Amanda Taylor, and Wenjing Li. 2021. Mental health apps for adolescents and young adults: A systematic review of randomised controlled trials. *Children and Youth Services Review* 127 (2021), 106073.

[40] Robert L Longyear and Kostadin Kushlev. 2021. Can mental health apps be effective for depression, anxiety, and stress during a pandemic? *Practice Innovations* 6, 2 (2021), 131.

[41] Kirsty Macmillan, Tessa Berg, Mike Just, and Mary Stewart. 2020. Are autistic children more vulnerable online? Relating autism to online safety, child wellbeing and parental risk management. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*. 1–11.

[42] Nora McDonald and Andrea Forte. 2020. The politics of privacy theories: Moving from norms to vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–14.

[43] Andrew McNeill, Pam Briggs, Jake Pywell, and Lynne Coventry. 2017. Functional privacy concerns of older adults about pervasive health-monitoring systems. In *Proceedings of the 10th international conference on pervasive technologies related to assistive environments*. 96–102.

[44] Supriya Misra, Valerie W Jackson, Jeanette Chong, Karen Choe, Charisse Tay, Jazmine Wong, and Lawrence H Yang. 2021. Systematic review of cultural aspects of stigma and mental illness among racial and ethnic minority groups in the United States: Implications for interventions. *American Journal of Community Psychology* 68, 3-4 (2021), 486–512.

[45] Mozilla. 2023. Mozilla Study: Data Privacy Labels for Most Top Apps in Google Play Store are False or Misleading. Retrieved September 13, 2023 from https://foundation.mozilla.org/en/privacynotincluded/articles/mozilla-study-data-privacy-labels-for-most-top-apps-in-google-play-store-are-false-or-misleading/

[46] John A Naslund and Kelly A Aschbrenner. 2019. Risks to privacy with use of social media: understanding the views of social media users with serious mental illness. *Psychiatric services* 70, 7 (2019), 561–568.

[47] Heather Saunders Cynthia Cox Nirmita Panchal, Matthew Rae and Robin Rudowitz. 2022. How Does Use of Mental Health Care Vary by Demographics and Health Insurance Coverage? *KFF* (2022).

[48] Kristen O'Loughlin, Martha Neary, Elizabeth C Adkins, and Stephen M Schueller. 2019. Reviewing the data security and privacy policies of mobile apps for depression. *Internet interventions* 15 (2019), 110–115.

[49] Matthew J Page, Joanne E McKenzie, Patrick M Bossuyt, Isabelle Boutron, Tammy C Hoffmann, Cynthia D Mulrow, Larissa Shamseer, Jennifer M Tetzlaff, Elie A Akl, Sue E Brennan, et al. 2021. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *International journal of surgery* 88 (2021), 105906.

[50] Achilleas Papageorgiou, Michael Strigkos, Eugenia Politou, Efthimios Alepis, Agusti Solanas, and Constantinos Patsakis. 2018. Security and privacy analysis of mobile health applications: the alarming state of practice. *Ieee Access* 6 (2018), 9390–9403.

[51] Lisa Parker, Vanessa Halter, Tanya Karliychuk, and Quinn Grundy. 2019. How private is your mental health app data? An empirical study of mental health app privacy policies and practices. *International journal of law and psychiatry* 64 (2019), 198–204.

[52] Emma M Parrish, Tess F Filip, John Torous, Camille Nebeker, Raeanne C Moore, and Colin A Depp. 2021. Are mental health apps adequately equipped to handle users in crisis? *Crisis: The Journal of Crisis Intervention and Suicide Prevention* (2021).

[53] Giancarlo Pasquini and Scott Keeter. 2022. At least four-in-ten U.S. adults have faced high levels of psychological distress during COVID-19 pandemic. *Pew Research Center* (2022).

[54] Adam Powell, Preeti Singh, John Torous, et al. 2018. The complexity of mental health app privacy policies: a potential barrier to privacy. *JMIR mHealth and uHealth* 6, 7 (2018), e9871.

[55] One Mind PsyberGuide. 2023. About One Mind PsyberGuide. Retrieved February 08, 2024 from https://onemindpsyberguide.org/about-psyberguide/

[56] One Mind PsyberGuide. 2023. One Mind PsyberGuide | A Mental Health App Guide. Retrieved November 27, 2023 from https://onemindpsyberguide.org/apps/

[57] One Mind PsyberGuide. 2023. Professional Reviewers | One Mind PsyberGuide. Retrieved February 08, 2024 from https://onemindpsyberguide.org/about-psyberguide/professional-reviewers/

[58] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J Aviv. 2019. " Woe is me" Examining Older Adults' Perceptions of Privacy. In *Extended abstracts of the 2019 CHI conference on human factors in computing systems*. 1–6.

[59] Daniel Reinhardt, Johannes Borchard, and Jörn Hurtienne. 2021. Visual Interactive Privacy Policy: The Better Choice?. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–12.

[60] Julie M Robillard, Tanya L Feng, Arlo B Sporn, Jen-Ai Lai, Cody Lo, Monica Ta, and Roland Nadler. 2019. Availability, readability, and content of privacy policies and terms of agreements of mental health apps. *Internet interventions* 17 (2019), 100243.

[61] Jessica N Rocheleau and Sonia Chiasson. 2022. Privacy and Safety on Social Networking Sites: Autistic and Non-Autistic Teenagers' Attitudes and Behaviors. *ACM Transactions on Computer-Human Interaction (TOCHI)* 29, 1 (2022), 1–39.

[62] Wulf Rössler. 2016. The stigma of mental disorders: A millennia-long history of social exclusion and prejudices. *EMBO reports* 17, 9 (2016), 1250–1253.

[63] Shruti Sannon and Andrea Forte. 2022. Privacy research with marginalized groups: what we know, what's needed, and what's next. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–33.

[64] Stephen M Schueller, Martha Neary, Jocelyn Lai, and Daniel A Epstein. 2021. Understanding people's use of and perspectives on mood-tracking apps: interview study. *JMIR mental health* 8, 8 (2021), e29368.

[65] Nelson Shen, Michael-Jane Levitan, Andrew Johnson, Jacqueline Lorene Bender, Michelle Hamilton-Page, Alejandro Alex R Jadad, David Wiljer, et al. 2015. Finding a depression app: a review and content analysis of the depression app marketplace. *JMIR mHealth and uHealth* 3, 1 (2015), e3713.

[66] Nelson Shen, Lydia Sequeira, Michelle Pannor Silver, Abigail Carter-Langford, John Strauss, and David Wiljer. 2019. Patient privacy perspectives on health information exchange in a mental health context: qualitative study. *JMIR mental health* 6, 11 (2019), e13306.

[67] Abigale Stangl, Kristina Shiroma, Bo Xie, Kenneth R Fleischmann, and Danna Gurari. 2020. Visual content considered private by people who are blind. In

Proceedings of the 22nd International ACM SIGACCESS Conference on Computers and Accessibility. 1–12.

[68] Katarzyna Stawarz, Chris Preist, Debbie Tallon, Nicola Wiles, and David Coyle. 2018. User experience of cognitive behavioral therapy apps for depression: an analysis of app functionality and user reviews. *Journal of medical Internet research* 20, 6 (2018), e10120.

[69] Colleen Stiles-Shields, Enid Montague, Emily G Lattie, Mary J Kwasny, and David C Mohr. 2017. What might get in the way: barriers to the use of apps for depression. *Digital Health* 3 (2017), 2055207617713827.

[70] Madiha Tabassum, Abdulmajeed Alqhatani, Marran Aldossari, and Heather Richter Lipford. 2018. Increasing user attention with a comic-based policy. In *Proceedings of the 2018 chi conference on human factors in computing systems*. 1–6.

[71] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. 2019. " I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)*. 435–450.

[72] Bill Toulas. 2023. Mental health provider Cerebral alerts 3.1M people of data breach. Retrieved September 13, 2023 from https://www.bleepingcomputer.com/news/security/mental-health-provider-cerebral-alerts-31m-people-of-data-breach/

[73] Leanne Townsend and Claire Wallace. 2016. Social media research: A guide to ethics. *University of Aberdeen* 1, 16 (2016).

[74] Lucy Van Kleunen and Stephen Voida. 2019. Challenges in supporting social practices around personal data for long-term mental health management. In *Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers*. 944–948.

[75] Rajesh Vasa, Leonard Hoon, Kon Mouzakis, and Akihiro Noguchi. 2012. A preliminary analysis of mobile app user reviews. In *Proceedings of the 24th Australian computer-human interaction conference*. 241–244.

[76] H Shellae Versey. 2022. Can mobile methods bridge psychology and place-based research? *Qualitative Psychology* 9, 2 (2022), 156.

[77] Yang Wang. 2017. The third wave? Inclusive privacy and security. In *Proceedings of the 2017 new security paradigms workshop*. 122–130.

[78] Dongsong Zhang, Jaewan Lim, Lina Zhou, and Alicia A Dahl. 2021. Breaking the Data Value-Privacy Paradox in Mobile Mental Health Systems Through User-Centered Privacy Protection: A Web-Based Survey Study. *JMIR Mental Health* 8, 12 (2021), e31633.

[79] Shikun Zhang, Yuanyuan Feng, Yaxing Yao, Lorrie Faith Cranor, and Norman Sadeh. 2022. How usable are ios app privacy labels? *UMBC Faculty Collection* (2022).

A APPENDIX

A.1 Supplementary Table

Table 2: MHAs Included in the Analysis

App Name	App Store	Number of User Reviews After Exclusion	Number of Relevant Reviews
Cerebral - Mental Health	Apple App Store, Google Play	927, 103	16, 13
Replika -Virtual AI Companion	Apple App Store, Google Play	1000, 430	29, 9
Youper - CBT Therapy Chatbot	Apple App Store, Google Play	902, 608	2, 26
BetterHelp - Therapy	Apple App Store, Google Play	1000, 625	10, 15
Sensa	Apple App Store, Google Play	396, 649	8, 15
Insight Timer - Meditation App	Apple App Store, Google Play	995, 281	17, 4
Headspace: Mindful Meditation	Apple App Store, Google Play	1000, 107	6, 11
7 Cups: Online Therapy & Chat	Apple App Store, Google Play	29, 579	9, 5
Breeze: Mental Health	Apple App Store, Google Play	772, 401	10, 3
Fabulous Daily Routine Planner	Apple App Store, Google Play	1000, 315	9, 4
Aura: Meditation & Sleep	Apple App Store, Google Play	837, 371	4, 6
Clarity - CBT Thought Diary	Apple App Store, Google Play	518, 417	8, 2
Ginger Emotional Support	Apple App Store, Google Play	388, 536	7, 3
Talkspace Counseling & Therapy	Google Play	694	10
Me+ Daily Routine Planner	Apple App Store	702	9
Mood Tracker Journal	Google Play	97	9
Bloom: CBT Therapy & Journal	Apple App Store	715	8
Calm	Apple App Store, Google Play	999, 169	3, 5
Daylio Journal - Daily Diary	Apple App Store	452	8
Feelsy: Stress Anxiety Relief	Apple App Store, Google Play	599, 519	2, 6
Inflow - Manage your ADHD	Apple App Store	241	8
Sanvello: Anxiety & Depression	Apple App Store, Google Play	556, 651	7, 1
stoic. journal & planner	Apple App Store	796	8
MindDoc: Your Companion	Apple App Store, Google Play	396, 266	2, 5
VOS: Wellbeing Plan & Journal	Google Play	281	7
Balance: Meditation & Sleep	Apple App Store, Google Play	831, 475	0, 6
Jumping Minds - Feel Better	Google Play	463	6
Woebot: Your Self-Care Expert	Apple App Store, Google Play	990, 586	2, 4
BetterMe: Mental Health	Apple App Store, Google Play	267, 310	1, 4
Breethe - Meditation & Sleep	Apple App Store, Google Play	565, 297	5, 0
MindShift CBT - Anxiety Relief	Apple App Store, Google Play	85, 112	4, 1
The Tapping Solution	Apple App Store, Google Play	686, 420	1, 4
NOCD: OCD Therapy and Tools	Apple App Store	70	4
PTSD Coach	Google Play	100	4
Rootd - Panic Attack Relief	Apple App Store	246	4
Sleep	Apple App Store	351	4
Remente: Self Care & Wellbeing	Apple App Store, Google Play	16, 404	0, 4
Wisdo: Mental Health & Support	Apple App Store, Google Play	80, 145	3, 1
29k: Mental Health & Wellbeing	Apple App Store, Google Play	45, 120	0, 3
AbleTo	Apple App Store, Google Play	36, 30	2, 1
How We Feel	Apple App Store	364	3
Journal Diary	Apple App Store	59	3
Loóna: calm, relax and sleep	Apple App Store	967	3
Silk + Sonder Guided Self-Care	Apple App Store	105	3
Reflectly - Journal & AI Diary	Apple App Store, Google Play	1000, 198	1, 2
ReGain - Couples Therapy	Apple App Store	537	3
Therapeer: Peer Support Groups	Apple App Store	143	3
Alan Mind Daily Journal	Apple App Store	391	2
Anxiety & Sleep: Urban Health	Google Play	151	2
being: my mental health 'map'	Google Play	528	2
DBT Coach : Guided Therapy	Google Play	60	2
Finch: Self Care Pet	Apple App Store, Google Play	1000, 519	1, 1
Medito: Meditation & Sleep	Apple App Store, Google Play	210, 113	2, 0
Mood Balance:Self Care Tracker	Apple App Store	492	2
Moodnotes - Mood Tracker	Apple App Store	267	2
Shmoody: Improve Your Mood	Apple App Store, Google Play	71, 361	1, 1
Sleep Sounds - relaxing sounds	Google Play	201	2
TalkLife	Apple App Store, Google Play	203, 694	2, 0

Table 3: MHAs Included in the Analysis Continue 1

App Name	App Store	Number of User Reviews After Exclusion	Number of Relevant Reviews
Amaha (InnerHour): self-care	Google Play	348	1
Anxiety Tracker-Log & Analyze	Google Play	81	1
Bearable - Symptom Tracker	Apple App Store	218	1
CBT Companion: Therapy App	Apple App Store, Google Play	58, 726	0, 1
Elomia: AI Therapy Chat	Apple App Store	44	1, 0
Evolve: Self-Care & Meditation	Google Play	456	1
Grid Diary - Journal, Planner	Apple App Store	54	1
HarmLess: Self Harm Tracker	Apple App Store	198	1
Humans Anonymous	Apple App Store	137	1
Intellect: Create A Better You	Google Play	135	1
Mind journal: Diary, Mood trac	Google Play	592	1
Mindbliss - Meditation & Sleep	Apple App Store	12	1
MindPeers- For Mental Strength	Google Play	420	1
MINDSET by DIVE Studios	Apple App Store, Google Play	674, 141	1, 0
Moodfit: Mental Health Fitness	Apple App Store, Google Play	88, 284	0, 1
MoodSpace - Stress, anxiety, &	Google Play	21	1
Neurocycle	Apple App Store	305	1
Nguvu Health: Therapy for all	Google Play	43	1
OCD.app - Anxiety Mood & Sleep	Apple App Store, Google Play	58, 41	0, 1
Pride Counseling	Apple App Store	135	1
Real: Mental Health	Apple App Store	52	1
Sleepiest: Sleep Meditations	Apple App Store	612	1
SOS Method: Stress & Anxiety	Google Play	418	1
ThoughtFullChat: Mental Health	Google Play	68	1
Wysa: Anxiety, therapy chatbot	Apple App Store, Google Play	637, 351	1, 0
Aetheria	Apple App Store	12	0
Amaru: Self-care Virtual Pet	Apple App Store	226	0
Better Sleep with KindMind	Apple App Store	20	0
Bold: CBT Therapy Journal	Apple App Store	29	0
buddhify - mindfulness meditation on the go	Apple App Store, Google Play	81, 361	0, 0
Callie: All-In-One Self Care	Apple App Store	61	0
Calm Harm – manage self-harm	Apple App Store, Google Play	55, 28	0, 0
Calm Urge: Self Harm Tracker	Apple App Store	72	0
CareMe Health - Mental Health	Google Play	340	0
Cheerly: Daily Wellness Game	Google Play	513	0
Dare: Anxiety & Panic Attacks	Apple App Store, Google Play	256, 314	0, 0
Deep Sleep with Andrew Johnson	Google Play	302	0
DiveThru	Apple App Store	36	0
eMoods Bipolar Mood Tracker	Apple App Store	70	0
Emotion Tracker : Self Care	Apple App Store	27	0
Flow - Depression treatment	Google Play	206	0
HeadHelp: Self Care & Vent	Apple App Store	238	0
Hector: AI Therapist/Therapy	Apple App Store	46	0
heyy, your mental health guide	Google Play	4	0
Hiwell Therapy & Mental Health	Google Play	36	0
HopeQure: Counseling & Therapy	Google Play	500	0
Iona: Mental Health Support	Google Play	350	0
JoyScore: Joy & Self-Care Tool	Apple App Store	51	0
Meomind - Listen to therapy	Google Play	352	0
Mindfulness Coach	Google Play	245	0
Mindfulness Meditation .	Apple App Store	507	0
Mindllama breathe to relax	Apple App Store	160	0
Mindshine: Mental Health Coach	Google Play	14	0
Mindspa: The Mental Health App	Google Play	30	0

Table 4: MHAs Included in the Analysis Continue 2

App Name	App Store	Number of User Reviews After Exclusion	Number of Relevant Reviews
Mood Journal: emotions tracker	Google Play	288	0
Moodistory - Emotion Tracker	Apple App Store	43	0
MoodKit	Apple App Store	29	0
MoodTools - Depression Aid	Google Play	414	0
MyPossibleSelf: Mental Health	Google Play	21	0
Norbu: Stress management	Google Play	402	0
Now&Me - Therapy, Counselling	Google Play	37	0
Numo: Cringe-Free ADHD App	Apple App Store	67	0
Online Therapy & Counseling	Google Play	25	0
Online therapy, emotional help	Google Play	34	0
Pi Journal: anxiety relief the	Google Play	203	0
PursueCare	Google Play	388	0
ShareSpace:Vent&Care Community	Google Play	49	0
Simple Habit: Meditation	Google Play	48	0
Skylight: Spiritual Self-Care	Google Play	201	0
Sleep Sounds - Relax Music	Google Play	142	0
Tellmi: Better Mental Health	Google Play	425	0
The Hopeful | Daily Self-Care	Apple App Store	308	0
uMore - mental health tracker	Google Play	32	0
Unmind	Google Play	39	0
Unwinding Anxiety®	Google Play	155	0
UP! - Depression, Bipolar & Bo	Google Play	141	0
Voice – Mental Health Guide	Google Play	238	0
What's Up? - Mental Health App	Apple App Store, Google Play	28, 109	0, 0
WhiteFlag Mental Health App	Google Play	77	0
WHY Emotional Support &Therapy	Google Play	38	0
WorryTree: Anxiety Relief CBT	Google Play	42	0
Zen: Guided Meditation & Sleep	Apple App Store	116	0

Table 5: Final Set of Inductive Codes

Theme	Subthemes	Codes
3rd party involvement		data selling to marketers, data sharing with partner without consent, data used for marketing, data sharing with third parties, data used for ads, data used for research, data sharing, data selling, government used, sharing data with third parties
Data safety	Mishandling data	hacking, data breach, data handled by people they don't know, data leaks, data stealing, data loss due to policty changes, privacy invaded by algorithms
	Lacking security measures	lacking encryption, lacking protection for minors, lacking security settings, blocked by anti-virus software, preying vulnerabilities, confidentiality
Data Type Collected	Data tracking	data tracking across other apps, anti-privacy tracker, invasive data tracking, invasive data monitoring, unnecessary data tracking, unauthorized data tracking
	Data collection	unnecessary data collection, invasive data collection, identifying data collection, more data collection due to policy changes
	Personal health information	Personal health information, hipaa violation
Agency	Ownership of the data	unable to access personal information, unable to cancel the account, unable to control data selling, unable to delete card information, unable to delete messages, unable to delete personal information, unable to edit personal information, unable to opt-out of emails, unable to delete entries, unable to remove partner from the account, unable to turn off data tracking
	Manipulative data practices	lack of transparency about data handling, lack of transparency about data storage, lack of transparency about data usage, unable to contact the company regarding privacy policy Deceptive data gathering: create an account, data storing, forced permission, mandatory data collection, not following thier policy Unethical data usage: data hostage, insurance fraud, unauthorized charges, under investigation, not following thier policy