REPORT

# Peace of Mind ...

## Evaluating the privacy practices of mental health apps

**Last updated: January 8th, 2021**

Stephanie Nguyen, Consumer Reports
Bill Fitzgerald, Consumer Reports
Bobby Richter, AppCensus
Justin Brookman, Consumer Reports

CR Consumer Reports | Digital Lab

# Table of Contents

**Acknowledgements**

This report was authored by Stephanie Nguyen, Bobby Richter, Justin Brookman and Bill Fitzgerald. In addition, there were many Consumer Reports experts who were involved in the creation of this report. Thanks to Thomas Germain, Ben Moskowitz, Cyrus Rassool, Camille Calman, Tim La Payne, Sharee McKenzie Taylor, Azad Yakatally, Daniela Nunez, Jerry Beilinson, Christina Tetreault, Amira Dhalla and others for valuable contributions. This report was originally published 12/17/20 and amended 12/18/20 and in January 2020. We also want to acknowledge the team at AppCensus, especially Bobby Richter and Serge Egelman, for contributing methodologies and analysis to better understand the hidden behaviors of mobile apps.

AppCensus

***Editor's note****: Earlier versions of this report included a chart summarizing a subset of the findings. While the general findings about CR's reading of the different apps' privacy policies remain, the chart has been removed to avoid any reader confusion that these mental health apps were being rated or ranked or that all these apps worked the same way. We have made other minor edits to reflect the removal of the chart.*

## Section 1. Executive summary

App-based mental health counseling is a growing industry, with some projecting a $3.9 billion category by 2027.[1] One major growth driver is the COVID-19 pandemic, which has triggered immense social, financial and economic impacts.[2] The pandemic has negatively affected many people's mental health and created barriers for access to help cope with mental illness and depression.[3]

Access to app-based mental health counseling may hold many benefits for consumers. However, applications that collect sensitive health information present new privacy risks. Breaches of or leakage consumers' sensitive health data can create negative, irreversible impacts on individuals including social stigmatization and barriers to access or future opportunities. Apps may collect sensitive, personally identifiable information about consumers and whether they suffer anxiety disorders, depression bipolar disorders, eating disorders, and post-traumatic stress disorders.

For these and other reasons, Consumer Reports conducted an evaluation of the privacy practices of 7 mental health apps: BetterHelp, MindDoc (formerly Moodpath), Sanity & Self, Talkspace, Wysa, Youper, and 7 Cups.

The Consumer Reports team analyzed these 7 apps using mixed methods, including data testing, a design (UX + UI) review and a policy review (inclusive of privacy policies and terms of service). Based on our report, we make four recommendations for providers of app-based mental health counseling:

> **Recommendation 1: Clearly explain procedures used for de-identification of data used for research. Identifiable data should not be shared except at the consumer's direction.** We advocate for companies to improve clarity on research for data sharing especially around how they define "anonymized data." Companies should be explicit about what processes they use to de-identify data. We highlight this to help prevent people from being reidentified. Mental health applications collect sensitive information that can create damaging, irreversible impacts on individuals if shared with third parties, including social stigmatization and additional barriers to future opportunities.

[1] Insights, Absolute Markets. *Mental Health Apps Market Accounted for US$ 587.9 Mn in 2018 and Is Expected to Generate a Revenue of US$ 3,918.40 Mn by 2027, at a Growth Rate of 23.7% from 2019 - 2027*. 3 Feb. 2020, www.prnewswire.com/news-releases/mental-health-apps-market-accounted-for-us-587-9-mn-in-2018-and-is-expected-to-generate-a-revenue-of-us-3-918-40-mn-by-2027--at-a-growth-rate-of-23-7-from-2019--2027--300997559.html.

[2] Nirmita Panchal, Rabah Kamal, and Apr 2020. "The Implications of COVID-19 for Mental Health and Substance Use." KFF, 21 Aug. 2020, www.kff.org/coronavirus-covid-19/issue-brief/the-implications-of-covid-19-for-mental-health-and-substance-use/.

[3] Syed, Kanwal, and Naitian Zhou. "Pandemic's Toll on Mental Health Accentuated in Cities." NBCNews.com, NBCUniversal News Group, 8 Dec. 2020, www.nbcnews.com/health/mental-health/map-anxiety-depression-your-state-compares-united-states-n1248473.

**Recommendation 2: Provide clear and contextually-appropriate explanations of how user-provided data will be used, so users are aware of potential consequences before they share.** Companies should not overwhelm people with superfluous information or choices. Wherever possible, app default settings should be that your privacy is protected and users should not have to worry about managing this on their own. However, if there are choices to be made or information someone should be aware of, they should be presented in a clear and straightforward way.

**Recommendation 3: Adhere to platform guidelines that are in place to protect people's privacy.** App developers should ensure that their apps meet the guidelines laid out in Android developer documentation, such as *Best Practices for Unique Identifiers* which recommends avoiding the use of identifiers like the Android ID (SSAID). App developers should also make sure that the libraries (SDKs) they embed within their apps meet their own expectations for data collection, and that they are configured accordingly.

**Recommendation 4: Transparently disclose the service providers that receive data when people use your apps.** We recommend that companies are more transparent in their privacy policies about the service providers that receive data. Although it is not legally required or common practice in the U.S. to list every service provider or institution receiving data, we recommend companies proactively disclose this information.

## Section 2. Context

**Mental health apps growing in popularity:** App-based mental health counseling is a large and growing industry. These apps accounted for $587.9 million in 2018 and are expected to generate up to $3.9 billion in annual revenue by 2027, according to some estimates. Due to greater awareness related to the significance of mental health, U.S. and Canadian consumers made up the majority of the global market in 2018.

**Increased anxiety and tumult, harms not evenly distributed:** Recent events like the global coronavirus pandemic, the resulting economic crisis, and large scale protests related to the Black Lives Matter movement, have spotlighted rising mental health related harms with marginalized and vulnerable populations. Increased anxiety and upheaval causes both physical and psychological symptoms and can be very distressing[4]. Since April, nearly half of Americans said the "pandemic was having a negative effect on their mental health," according to a survey[5] by the

[4] "Symptoms, Signs, and Side Effects of Anxiety." Medical News Today, MediLexicon International, www.medicalnewstoday.com/articles/322510.

[5] Ashley Kirzinger @AshleyKirzinger on Twitter. "KFF Health Tracking Poll – Early April 2020: The Impact Of Coronavirus On Life In America." KFF, 20 Apr. 2020, www.kff.org/health-reform/report/kff-health-tracking-poll-early-april-2020/.

Kaiser Family Foundation. Moreover, recent Census Bureau research[6] has shown that anxiety and depression spiked for black and Asian Americans after George Floyd was killed by the police. An annual report from Safe2Say[7] noted that in Pennsylvania schools, an "increased portion of the calls, online tips and other reports that did come in were for issues of suicidal thoughts or self-harm", data from the system showed.[8] Finally, the pandemic has exposed disparities in the U.S. mental health system, reported the Center for American Progress.[9] People with mental health disabilities face "disproportionately high rates of poverty[10]", "housing and employment discrimination[11]", and criminalization.[12] In addition to the services evaluated in this report, numerous app-based mental health counseling features[13], as well as niche apps, are drawing a "wave of new users[14]." For instance, to remove the stigma attached with mental health challenges among the Black community, Jasmin Pierre created "The Safe Place," a mental health app to bring more awareness, education, and hope in ways that are tailored to the black community.

**Data leaks:** In addition to rising harms with communities of color and youth, there are numerous documented data leaks with mental health applications. Investigative journalists have highlighted issues around excessive data sharing due to allegedly flawed business models[15] with the argument that apps can either sell subscriptions to services or sell data. Some have called for enhanced and more stringent regulation[16] on these apps, marketed to people with anxiety, autism and depression. Other research highlighted how "the majority of the top-ranked mental health apps for depression and smoking cessation" share user data without disclosing the practice in

[6] Fowers, Alyssa, and William Wan. "Depression and Anxiety Spiked among Black Americans after George Floyd's Death." The Washington Post, WP Company, 12 June 2020, www.washingtonpost.com/health/2020/06/12/mental-health-george-floyd-census/?arc404=true.

[7] Shapiro, Josh. Safe2Say Something Annual Report. Safe2Say, 30 June 2020, www.attorneygeneral.gov/wp-content/uploads/2020/08/2019-2020-S2SS-Annual-Report-FINAL.pdf.

[8] Press, The Associated. "More Calls about Self-Harm, Suicidal Thoughts Made to Pa. Schools Hotline after Quarantine." Pennlive, 8 Aug. 2020, www.pennlive.com/news/2020/08/more-calls-about-self-harm-suicidal-thoughts-made-to-pa-schools-hotline-after-quarantine.html.

[9] Rapfogel, Azza Altiraifi and Nicole. "Mental Health Care Was Severely Inequitable, Then Came the Coronavirus Crisis." Center for American Progress, www.americanprogress.org/issues/disability/reports/2020/09/10/490221/mental-health-care-severely-inequitable-came-coronavirus-crisis/.

[10] "SERIOUS MENTAL ILLNESS AMONG ADULTS BELOW THE POVERTY LINE." Serious Mental Illness Among Adults Below the Poverty Line, www.samhsa.gov/data/sites/default/files/report_2720/Spotlight-2720.html.

[11] U.S. Department of Housing and Urban Development. *Rental Housing Discrimination on the Basis of Mental Disabilities: Results of Pilot Testing*. Aug. 2017, www.huduser.gov/portal/sites/default/files/pdf/MentalDisabilities-FinalPaper.pdf.

[12] Ben-Moshe, Liat. "Disabling Incarceration: Connecting Disability to Divergent Confinements in the USA - Liat Ben-Moshe, 2013." SAGE Journals, journals.sagepub.com/doi/abs/10.1177/0896920511430864.

[13] Perez, Sarah. "TikTok Expands Community Guidelines, Rolls out New 'Well-Being' Features." TechCrunch, TechCrunch, 15 Dec. 2020, techcrunch.com/2020/12/15/tiktok-expands-community-guidelines-rolls-out-new-well-being-focused-features/.

[14] Herzog, Kira. "Mental Health Apps Draw Wave of New Users as Experts Call for More Oversight." CNBC, CNBC, 24 May 2020, www.cnbc.com/2020/05/24/mental-health-apps-draw-wave-of-users-as-experts-call-for-oversight.html.

[15] Becker, Rachel. "That Mental Health App Might Share Your Data without Telling You." The Verge, The Verge, 20 Apr. 2019, www.theverge.com/2019/4/20/18508382/apps-mental-health-smoking-cessation-data-sharing-privacy-facebook-google-advertising.

[16] "Privacy Concerns about Mental Health Apps Highlight Need for Regulation: Spectrum: Autism Research News." Spectrum, 5 Nov. 2019, www.spectrumnews.org/news/mental-health-apps-highlight-need-for-regulation/.

privacy policies.[17] When information about one's mental health data leaks, the tangible impact is that it might lead to higher insurance rates or job discrimination.[18]

Health apps are generally unregulated and are not covered by medical privacy laws.  The Health Insurance Portability and Accountability Act (HIPAA) provides some federal privacy protections for data you share with your doctor. However, those rules don't always apply to applications you can download to your phone. Consumer protection law prevents companies from lying to you about what they do with your data, but privacy disclosures are often vague and confusing, and are buried in privacy policies that few consumers have the time or training to parse.

CR previously evaluated[19] the privacy practices of women's reproductive health tracker apps. According to some of those findings, none of the five apps guaranteed that user collected information would be used in the ways they intended. All of the apps shared user data with third-party partners for purposes such as targeted advertising, which may share or reshare information to other third parties. While there were no major security issues, there were "shortcomings among all five apps in how they protect the sensitive data they gather," the reports cited.[20]

Previous CR research into mobile applications' data practices has led to enforcement actions for regulators. In September 2020, California Attorney General Xavier Becerra announced a "landmark settlement" with Glow Inc., which is a company that offers period tracking for fertility and health monitoring. Glow Inc. agreed to pay $250,000 to resolve a serious data privacy and security issue which put "women's personal and medical data at risk," Becerra's office said in a statement.[21] In addition to the civil penalty, Glow would need to comply with state consumer protection and privacy laws in order to get Glow to better consider how privacy or security breaches may uniquely impact women through their application. "Health apps have access to incredibly sensitive information about us and too often fail to take the most rudimentary of protections," explained Justin Brookman, Director of Privacy at Consumer Reports said. "Especially with CCPA in effect, the California Attorney General's office is at the front line of protecting our privacy and security—but rules are meaningless without robust enforcement, so this action is a promising sign."

[17] Davis, Jessica. "Mental Health Apps May Share User Data without Clear Privacy Policies." HealthITSecurity, HealthITSecurity, 26 June 2019, healthitsecurity.com/news/mental-health-apps-may-share-user-data-without-clear-privacy-policies.

[18] Singer, Natasha. "When Apps Get Your Medical Data, Your Privacy May Go With It." The New York Times, The New York Times, 3 Sept. 2019, www.nytimes.com/2019/09/03/technology/smartphone-medical-records.html.

[19] Rosato, Donna. "What Your Period Tracker App Knows About You." Consumer Reports, www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you/.

[20]Rosato, Donna. "What Your Period Tracker App Knows About You." Consumer Reports, www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you/.

[21]"Attorney General Becerra Announces Landmark Settlement Against Glow, Inc. – Fertility App Risked Exposing Millions of Women's Personal and Medical Information." State of California - Department of Justice - Office of the Attorney General, 21 Sept. 2020, oag.ca.gov/news/press-releases/attorney-general-becerra-announces-landmark-settlement-against-glow-inc-%E2%80%93.

## Section 3. Methods

We started our research by aggregating 25 mental health and meditation apps. We created a set of criteria to narrow this list including:

- **App usage**: Sorted by highest app usage according to Google Play and comScore.
- **Sharing of personal identifiers:** additional focus was given to apps that shared multiple identifiers with third parties.
- **Diversity of audience**: In addition to top apps, we included apps designed to cater to more specific users (e.g., Sanity & Self are focused on teen women, apps focused on curbing self harm / suicide, etc.).

Based on these criteria, we narrowed in on seven mental health applications for a complete evaluation: BetterHelp, MindDoc (formerly Moodpath), Sanity & Self, Talkspace, Wysa, Youper, and 7 Cups.

We used a number of methods to evaluate the privacy practices of these apps: 1) data testing, 2) design analysis, and 3) policy review.

**(1) Data Testing:** We ran a static analysis of each Android application. We also worked with AppCensus,[22] a company that analyzes app behavior for privacy and security issues, to do an automated analysis of the apps. This research process involved an inspection of the following items:

- Permissions: What access to data and features was requested, and what was actually used?
- Third Party SDKs: What third-party software is bundled with the app when a user installs it, and what role does it play in app behavior?
- Data recipients: Which entities (companies, services, etc.) receive information from the app, and which security and privacy methods / policies do they observe or not
- Personal information: What identifiers (Android ID, Advertising ID, etc.) from the phone are transmitted by the app, and where are these identifiers sent?
- We used the following Android app binaries:
    - BetterHelp[23] version 1.63
    - MindDoc[24] version 4.2.0

[22] AppCensus, www.appcensus.io/.
[23] “BetterHelp: Online Counseling &amp; Therapy - Apps on Google Play.” Google, Google, play.google.com/store/apps/details?id=com.betterhelp.
[24] “MindDoc: Mood Tracker for Depression &amp; Anxiety - Apps on Google Play.” Google, Google, play.google.com/store/apps/details?id=de.moodpath.android.

    - Sanity & Self[25] version 3.0.6396
    - Talkspace[26] version 3.30.80
    - Wysa[27] version 2.4.1
    - Youper version 8.04.000
    - 7 Cups[28] version 4.6.9

**(2) Design analysis (UX + UI):** The user experience, user interface design analysis involved a manual, thorough review of all of the user-interfacing elements of the applications. More specifically, the purpose of this work is to:

- Show how the company empowers and informs users, in support of and/or beyond what they say in the documents (Terms of Service and Privacy Policy).
- Understand how the app works, who this is positioned to.
- Understand how privacy / security are integrated and positioned (including privacy policy and terms of service documentation), including app defaults and permissions.
- Identify what the core components of the application featured are in order to do more testing, where necessary.
- Identify areas for sensitive data collection, and potentially cross reference that with app data collection and 3rd party sharing happening simultaneously.
- Capture which app permissions are requested, and if/when these permissions are accessed while using the app.
- We used the following iOS app versions:
    - BetterHelp: iOS app version 9.7[29]
    - MindDoc: iOS app version 4.2.1[30]
    - Sanity & Self: iOS app version 3.0.6502.180[31]
    - Talkspace: iOS app version 8.86.00[32]
    - Wysa: iOS app version 5.7.4[33]

[25] “Sanity &amp; Self: Anxiety Stress Relief, Sleep Sounds - Apps on Google Play.” Google, Google, play.google.com/store/apps/details?id=cc.moov.five.

[26] “Talkspace Counseling &amp; Therapy - Apps on Google Play.” Google, Google, play.google.com/store/apps/details?id=com.talkspace.talkspaceapp.

[27] “Wysa: Stress, Depression &amp; Anxiety Therapy Chatbot - Apps on Google Play.” Google, Google, play.google.com/store/apps/details?id=bot.touchkin.

[28] “7 Cups: Anxiety &amp; Stress Chat - Apps on Google Play.” Google, Google, play.google.com/store/apps/details?id=com.sevencupsoftea.app.

[29] BetterHelp. “BetterHelp - Online Counseling.” App Store, 10 July 2015, apps.apple.com/us/app/betterhelp-online-counseling/id995252384.

[30] GmbH, MindDoc Health. “MindDoc: Depression &amp; Anxiety.” App Store, 10 Nov. 2015, apps.apple.com/us/app/minddoc-depression-anxiety/id1052216403.

[31] Inc., Moov. “Sanity &amp; Self: Stress Relief.” App Store, 28 Oct. 2017, apps.apple.com/us/app/sanity-self-stress-relief/id1274153663.

[32] inc., Groop Internet Platform. “Talkspace Therapy &amp; Counseling.” App Store, 10 July 2013, apps.apple.com/us/app/talkspace-therapy-counseling/id661829386.

[33] Touchkin. “Wysa: Mental Health Support.” App Store, 22 Oct. 2016, apps.apple.com/us/app/wysa-mental-health-support/id1166585565.

- Youper: iOS app version 9.00.000[34]
- 7 Cups: iOS app version 4.6.9[35]

**(3) Policy review:** Third, the team reviewed the privacy policy and terms of service documents of the applications. We referred to the following privacy policies:

- BetterHelp, updated on September 11, 2020[36]
- MindDoc, no update date, reviewed on November 23, 2020[37]
- Sanity & Self, updated on January 31, 2020[38]
- Talkspace, updated on January 1, 2020[39]
- Wysa, updated on November 19, 2020[40]
- Youper, updated on February 20, 2020[41]
- 7 Cups, updated on May 15, 2020[42]

## 3.1 Research limitations

- **Findings are not necessarily unique to mental health.** First, many of our observations apply broadly to the mobile app ecosystem and are not necessarily unique to mental health apps. Many app designs and data sharing behaviors that have been well documented in other analyses and investigations—including research previously conducted by Consumer Reports and AppCensus, such as Consumer Reports' period tracker investigation[43], as well as AppCensus's review of the Australian Android App ecosystem.[44] We chose to still present these findings as they are important to establish current norms in data-collecting apps and norms that could be further identified and strengthened—especially given the sensitive nature of data collected by mental health apps.

- **Privacy policies and other disclosures are a limited source of information about consumer data protections.** As acknowledged in section 2, the lack of strong consumer

[34] Youper, Inc. "Youper: Self Care Therapy." App Store, 10 Jan. 2016, apps.apple.com/us/app/youper-self-care-therapy-chat/id1060691513.
[35]Tea, 7 Cups of. "7 Cups: Anxiety &amp; Stress Chat." App Store, 11 Oct. 2014, apps.apple.com/us/app/7-cups-anxiety-stress-chat/id921814681.
[36] "Privacy Policy." BetterHelp, www.betterhelp.com/privacy.
[37] "Privacy and Security Policy - Moodpath." MindDoc, mymoodpath.com/en/privacy-policy/.
[38] "Privacy." Sanity & Self, www.sanityandself.com/privacy/.
[39] "Privacy Policy." Talkspace, www.talkspace.com/public/privacy-policy.
[40] Wysa Privacy Policy, legal.wysa.io/privacy-policy.
[41] "Privacy Policy." Youper, 10 Sept. 2020, www.youper.ai/privacy-policy.
[42]"Privacy Policy" 7 Cups, www.7cups.com/Documents/PrivacyPolicy/.
[43] Rosato, Donna. "What Your Period Tracker App Knows About You." Consumer Reports, www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you/.
[44]Bobby Richter. "Snapshot of Privacy Behaviors in the Australian Android App Ecosystem." The AppCensus Blog, 18 Nov. 2020, blog.appcensus.io/2020/11/18/snapshot-of-privacy-behaviors-in-the-australian-android-app-ecosystem/.

privacy protections online means that many health apps are not subject to medical privacy laws. It is possible that some apps may be subject to obligations under the HIPAA when they connect users to licensed therapists. Conversely, apps that are not subject to HIPAA rules may publish privacy disclosures that are vague and incomplete—or confusingly advertise themselves as "HIPAA compliant."

- **Apps are constantly changing.** Within the span of just over three months (August to November 2020), several of the apps changed their privacy policies, terms of service, and app designs and user interfaces. One of the apps (Moodpath) rebranded to MindDoc. In addition, one of the apps (Youper) deleted their Android app, precluding our team from completing some of the testing that we conducted for the other apps. Our team did due diligence to increase the integrity of the findings.

- **Testing apps provides an imperfect snapshot-in-time.** We refreshed all of the findings in this report in late November 2020, closer to the time of this report's release. However, it is possible that the apps have changed some of these documented elements since we documented and published this work. Because apps are ultimately compilations of code, libraries, and services, it is difficult to ensure that every corner of an app is explored to its fullest. In that respect, these results may include false negatives: just because a specific app behavior was not observed does not mean the app is not capable of exhibiting that behavior in other circumstances. Developers do their best to protect their code and their data using various methods, some of which might still thwart our attempts to analyze them.

- **More complete picture of Android app behavior than iOS**. The Android and iOS operating systems are fundamentally different. Because Android is an open source project, it is easier to modify the system to facilitate privacy and data security testing.[45] The apps analysis carried out by AppCensus was therefore conducted using Android versions of each app.

- **Design review does not give us complete information to understand a company's intent (or lack thereof).** This process intends to highlight the presence of information to the end user and what that may imply in terms of positive or negative outcomes. However, many times, we do not know the details to make any judgments or inferences due to the number of unknown details. In the case of this report, especially in section 4.2, we highlight what UX and UI elements we observed through an analysis across the seven mental health apps. For instance, the presence of a "delete account" button in the mobile

[45] "Open-Source Software." Wikipedia, Wikimedia Foundation, 11 Dec. 2020, en.wikipedia.org/wiki/Open-source_software.

app settings page implies that the user can easily delete their information. However, this alone still requires follow up and investigation to better understand the parameters and definitions behind the user interface element. For illustration: does a “delete data” function technically mean that the app deletes someone’s data immediately, or after seven years as is stated in the privacy policy? If the “delete account” button points the user toward a CCPA specific page, which only applies to California residents, does someone in Virginia get to use the same privileges of deleting their account as a California resident? Sometimes, with lack of answers in the user interface, public documentation (e.g., a website or app store profile), or privacy policies, Consumer Reports will directly reach out to the companies for answers. We sought comments from companies in some cases where the answers were not apparent from a review of the application’s UX or UI design or policy documents.

# Section 4. Findings

## 4.1 Data Testing

Our automated analysis of the apps included an audit of app permissions, third party SDKs, data recipients, and transmitted identifiers (personal or device). This approach allows us to see how data is collected, where it goes, and potentially infer why it goes there. In December 2020, we followed up on research originally conducted in August 2020. As noted in 3.1, since the Youper app is no longer offered for Android, this precluded our ability to re-test its data collection and sharing components.

We outline key findings from this research:

### 4.1.1 - In general, the applications we examined sent specific identifiers to multiple third parties. While this is not atypical of mobile apps, one would hope or expect that mental health apps would be especially protective of user privacy. Our testing showed nearly all apps sending the Advertising ID—which is used for advertising and analytics[46]—with some apps pairing the Advertising ID with the Android ID.

- We observed MindDoc sending the Android Advertising ID (AAID) and Android ID to Branch within the same transmission. Google's developer guidelines clearly recommend against allowing the Advertising ID to be linked to other sensitive or persistent identifiers, unless a user has given explicit consent.
- We observed transmissions of the Android ID from Wysa to graph.facebook.com and api2.branch.io. Wysa’s privacy policy discloses that Wysa uses these services for

[46] “Ads - Play Console Help.” Google, Google, support.google.com/googleplay/android-developer/answer/9857753.

analytics; however, for analytics, we would expect this ID to be the Advertising ID, since users can control tracking to some degree by resetting the Advertising ID in Android's ad settings.

- We also observed transmissions of the Advertising ID and Android ID from Sanity & Self to Crashlytics (settings.crashlytics.com) within the same transmission. Google's developer guidelines clearly recommend against allowing the Advertising ID to be linked to other sensitive or persistent identifiers, unless a user has given explicit consent. The terms of Sanity & Self do not contain clear language describing consent mechanisms that would permit bridging IDs.

| MindDoc to Branch | Sanity & Self to Crashlytics |
|---|---|
| POST /v1/close HTTP/1.1<br>Content-Type: application/json<br>Accept: application/json<br>User-Agent: <REDACTED><br>Host: api2.branch.io<br>Connection: Keep-Alive<br>Accept-Encoding: gzip<br>Content-Length: 727<br><br>{"device_fingerprint_id":"<REDACTED>","identity_id":"<REDACTED>","session_id":"<REDACTED>","app_version":"4.2.0","hardware_id":"<ANDROIDID>","is_hardware_id_real":true,"brand":"Google","model":"AOSP on sargo","screen_dpi":440,"screen_height":2088,"screen_width":1080,"wifi":true,"ui_mode":"UI_MODE_TYPE_NORMAL","os":"Android","os_version":28,"language":"en","local_ip":"<REDACTED>","metadata":{},"advertising_ids":{"aaid":"<AAID>"},"lat_val":0,"google_advertising_id":"<AAID>","instrumentation":{"v1\/close-qwt":"4","v1\/install-brtt":"493"},"sdk":"android5.0.3","branch_key":"<REDACTED>","retryNumber":0} | GET /spi/v2/platforms/android/apps/cc.moov.five/settings?instance=<REDACTED>&build_version=6396&display_version=3.0.6396&source=1&icon_hash=<REDACTED> HTTP/1.1<br><br>User-Agent: Crashlytics Android SDK/1.3.17.dev<br>X-CRASHLYTICS-DEVELOPER-TOKEN: <REDACTED><br>X-CRASHLYTICS-API-KEY: <REDACTED><br>X-CRASHLYTICS-API-CLIENT-TYPE: android<br>X-CRASHLYTICS-API-CLIENT-VERSION: 1.3.17.dev<br>Accept: application/json<br>X-CRASHLYTICS-DEVICE-MODEL: Google/AOSP on sargo<br>X-CRASHLYTICS-OS-BUILD-VERSION: <REDACTED><br>X-CRASHLYTICS-OS-DISPLAY-VERSION: 9<br>X-CRASHLYTICS-ADVERTISING-TOKEN: <AAID><br>X-CRASHLYTICS-INSTALLATION-ID: <REDACTED><br>X-CRASHLYTICS-ANDROID-ID: <ANDROIDID><br>Host: settings.crashlytics.com<br>Connection: Keep-Alive<br>Accept-Encoding: gzip |

### 4.1.2 - Privacy policy disclosures do not parallel the actions of these applications. This means it's hard to hold companies accountable for their data practices and to understand exactly what happens with your data.

In the privacy policy review, we sought to answer the following question: "Does the app name any of the companies they share your data with?" We found that the following apps did not list any third-party companies: 7 Cups, BetterHelp, Talkspace and Youper. The following apps did mention third party companies: MindDoc, Sanity & Self, and Wysa.

| App | Lists Third Party Companies in Privacy Policy |
|---|---|

| | |
|---|---|
| **7 Cups** | No |
| **BetterHelp** | No |
| **MindDoc** | Yes |
| **Sanity & Self** | Yes |
| **Talkspace** | No |
| **Wysa** | Yes |
| **Youper** | Unclear (No Android App at time of testing) |

To check these points, the CR team worked with AppCensus to look at the third parties contacted by these applications in order to answer the question: “Did we see the app share data ONLY with the companies named in the privacy policy?” For BetterHelp, MindDoc, Sanity & Self, Talkspace, Wysa, and Youper, the answer was no. (We note that for 7 Cups, the Terms of Service mentioned third-party cookies, but both static and dynamic analysis did not show any calls to third parties. It's unclear if this is intentional, whether the company is reserving the right to use third parties in the future, whether transmission takes place after collected by first-party services, or whether the policy refers to behavior of the website or other part of the business.

For the apps that named companies, we show what they disclosed in the privacy policies versus what we found with testing:

| | MindDoc (formerly Moodpath) | Sanity & Self | Wysa |
|---|---|---|---|
| **What third parties does the app mention they share data with in their policies?** | Google Firebase Crashlytics<br>Google Firebase Remote Config<br>Branch Metrics<br>Mailgun | Google Analytics<br>Apple Healthkit | Google Analytics, Facebook Analytics, Firebase, and Branch.io |
| **Third parties we detected through static analysis. Not all third parties listed may be in use.** | Google Analytics<br>Google CrashLytics<br>Google Firebase Analytics | AppsFlyer<br>Facebook Analytics<br>Facebook Login<br>Facebook Places<br>Facebook Share<br>Google AdMob<br>Google CrashLytics<br>Google Firebase Analytics<br>Instabug<br>MixPanel | Google CrashLytics<br>Google Firebase Analytics |
| **Third parties to which we observed transmissions to during app testing**<br>(White highlights indicate personal/device identifiers observed in transmissions) | **Branch**<br>api2.branch.io<br>cdn.branch.io<br>**Google Firebase**<br>firebase-settings.crashlytics.com<br>firebaseinstallations.googleapis.com<br>firebaseremoteconfig.googleapis.com | **Instabug**<br>api.instabug.com<br>**MixPanel**<br>api.mixpanel.com<br>decide.mixpanel.com<br>**AppsFlyer**<br>conversions.appsflyer.com<br>gcdsdk.appsflyer.com<br>register.appsflyer.com<br>**Facebook**<br>graph.facebook.com<br>**Google Firebase**<br>ctalias2015.firebaseio.com<br>firebaseremoteconfig.googleapis.com<br>**Google Cloud Storage**<br>release-assets-moov-cc.storage.googleapis.com<br>storage.googleapis.com<br>**Google Crashlytics**<br>settings.crashlytics.com | **Branch**<br>api2.branch.io<br>cdn.branch.io<br>**Facebook**<br>graph.facebook.com<br>scontent-sjc3-1.xx.fbcdn.net<br>**Google Crashlytics**<br>firebase-settings.crashlytics.com<br>**Google Firebase**<br>firebaseinappmessaging.googleapis.com<br>firebaseinstallations.googleapis.com<br>firebaseremoteconfig.googleapis.com |

By contrast, the privacy policy for TalkSpace mentions two third parties: Facebook and Twitter. However, during app testing we observed data being sent to five different companies: Mixpanel, Appsflyer, Facebook, New Relic, and Braze.

## 4.2 UX + UI Design Review

### Dark Patterns: UX + UI Design Highlights

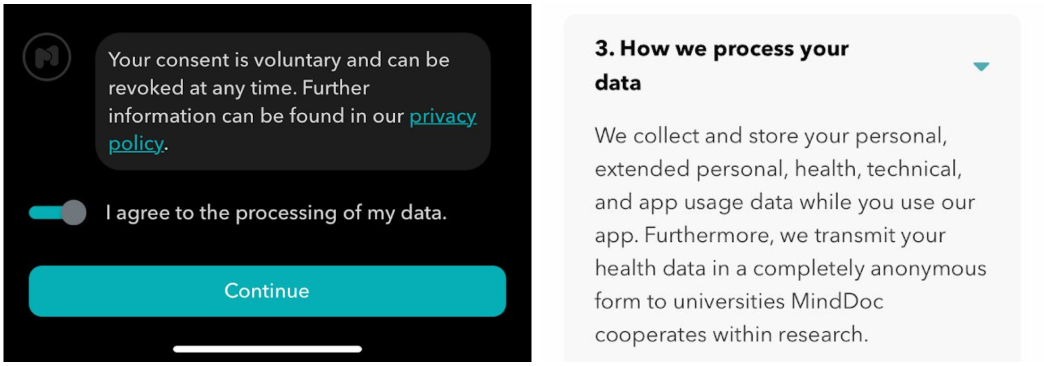
We highlight some themes of dark patterns, defined as “user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions,” by Princeton University researchers. The 4 patterns we highlight and explain in detail below are the following:

- 4.2.1 - Companies may opt users into academic research by default or do it in a way that is not clearly outlined or articulated to the user.
- 4.2.2 - Some companies make elements of the user profile public by default.
- 4.2.3 - Several apps took different approaches to allowing users to delete their data easily through the mobile app interface.
- 4.2.4 - Companies may encourage mental health app users to share data in communities without clear disclosures in the app design and user interface that comments may be shared with the public.

### 4.2.1 - Companies may opt users into academic research by default or do it in a way that is not clearly outlined or articulated to the user.

- 2 of the apps share data for research (MindDoc, Youper).
- 1 of them (MindDoc) incorporates “consent” in an unclear way.

For example, MindDoc (formerly Moodpath) uses language “processing of data” to mean they will share user data for academic research to several institutions. MindDoc asks users to “agree to the processing of my data” through the chat’s user interface function. Processing of data translates into practice as giving MindDoc consent to automatically transmit health data to research partners and universities. While MindDoc claims to share "anonymous data," there is no description of what they mean by that term, either presented to the user or in privacy documentation.



Your consent is voluntary and can be revoked at any time. Further information can be found in our privacy policy.

I agree to the processing of my data.

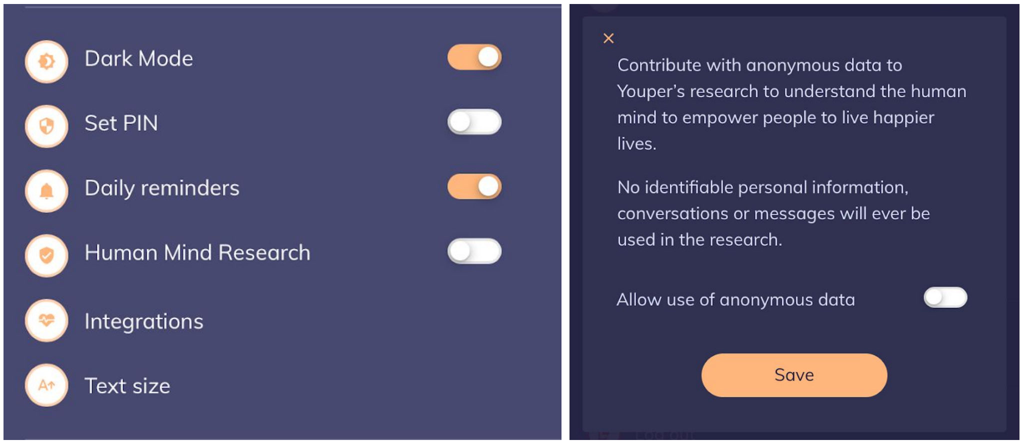
Continue

**3. How we process your data**

We collect and store your personal, extended personal, health, technical, and app usage data while you use our app. Furthermore, we transmit your health data in a completely anonymous form to universities MindDoc cooperates within research.

*Figure 1: MindDoc's chatbot references the image on the left. When the user clicks on "privacy policy" and scrolls to "How we process your data" they are given text displayed on the image on the right.*

In Youper's setting page, the "Human Mind Research" toggle is OFF by default. When clicked, there is a pop-up that explicitly explains, "Contribute with anonymous data to Youper's research to understand the human mind to empower people to live happier lives. – No identifiable personal information, conversations or messages will ever be used in the research. – Allow use of anonymous data." There is clear language that allows users to opt-in instead of opt-out of sharing anonymous data through the app by default.



Dark Mode

Set PIN

Daily reminders

Human Mind Research

Integrations

Text size

Contribute with anonymous data to Youper's research to understand the human mind to empower people to live happier lives.

No identifiable personal information, conversations or messages will ever be used in the research.

Allow use of anonymous data

Save

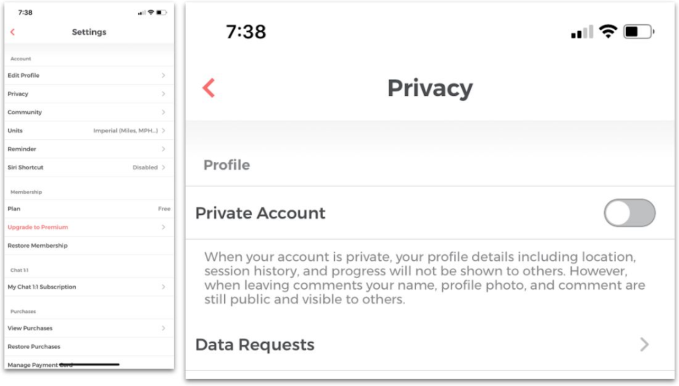
*Figure 2: Youper's setting page highlights that "Human Mind Research" is OFF by default.*

### 4.2.2 - Some companies make elements of the user profile public by default.

- 2 of the apps are affiliated with a community. (Sanity & Self and 7 Cups).
- 1 of the apps (for teen girls) made the app public by default in the settings page (see image below).

Sanity & Self highlights the ability for a user to make a "private account" off or on by default.

When we checked on August 27, 2020 and again on November 26, 2020, Sanity & Self (an app positioned for teen girls) had the “private account” setting as OFF by default (screenshot below) in the iOS app v3.0.6502.180. The app defines that turning this toggle ON means “When your account is private, your profile details including location, session history, and progress will not be shown to others. However, when leaving comments your name, profile photo, and comment are still visible to others.” Apps, especially those geared toward younger teen girls should NOT share profile details including location, session history, and progress by default.



7:38

Settings

Account

Edit Profile

Privacy

Community

Units Imperial (Miles, MPH...)

Reminder

Siri Shortcut Disabled

Membership

Plan Free

Upgrade to Premium

Restore Membership

Chat 1:1

My Chat 1:1 Subscription

Purchases

View Purchases

Restore Purchases

Manage Payment Card

7:38

Privacy

Profile

Private Account ○

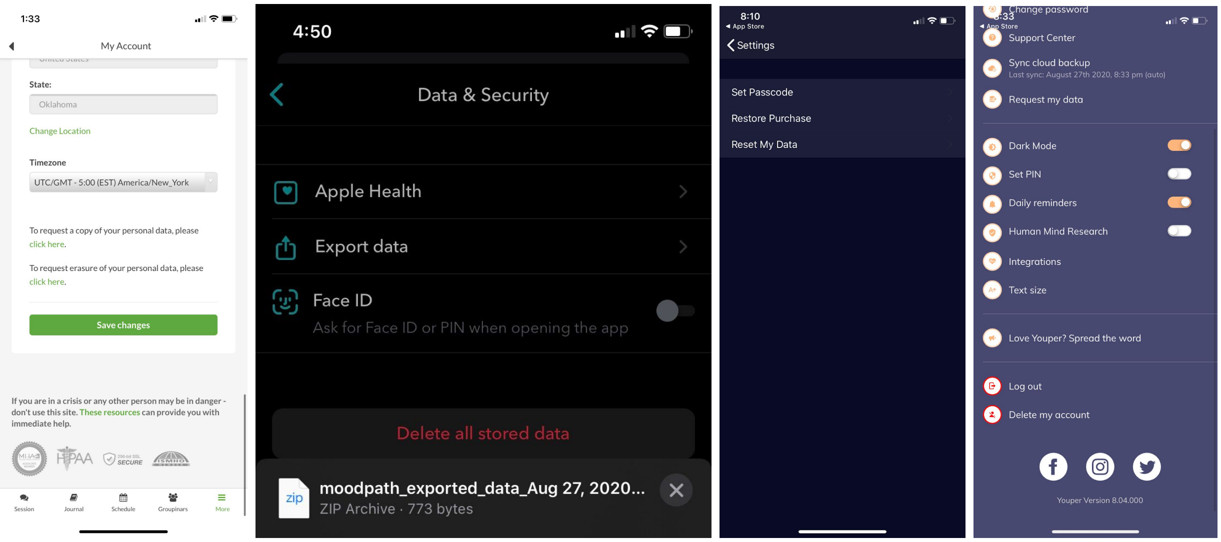
When your account is private, your profile details including location, session history, and progress will not be shown to others. However, when leaving comments your name, profile photo, and comment are still public and visible to others.

Data Requests

*Figure 3: Sanity & Self’s Privacy Page features a “Private Account” setting that users can toggle on and off.*

### 4.2.3 - Several apps took different approaches to allowing users to delete their data easily through the mobile app interface.

4 of 7 apps - Four apps including BetterHelp, MindDoc, Wysa, and Youper offered methods to delete your account or data through the settings page, one only highlighted the feature for California residents due to CCPA, and two apps did not offer any option to delete the account or user data.



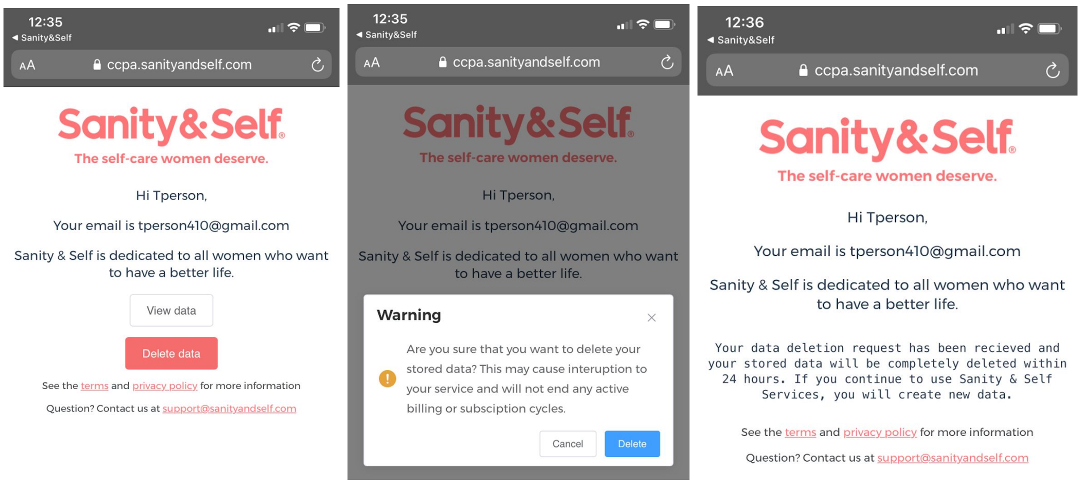
To request a copy of your personal data, please click here.

To request erasure of your personal data, please click here.

If you are in a crisis or any other person may be in danger - don't use this site. These resources can provide you with immediate help.

*Figure 4: [From left to right] BetterHelp, MindDoc, Wysa and Youper's settings page offer methods to delete your account or data through the user interface*

1 of 7 apps, Sanity & Self, has a button labeled "Delete Data" through the app, but this link goes to "https://ccpa.sanityandself.com/ccpa?", which are legal rights in the privacy policy that are specified for only California residents related to the California Consumer Privacy Act (CCPA), as opposed to being an option for all users to delete their data. However, during the mobile test our team conducted—not in California—we were able to seemingly delete the user account through the mobile interface. Upon trying to log in after clicking the "Delete Data" button and then another "Delete" button, we were unable to log in using the previous account.



Hi Tperson,

Your email is tperson410@gmail.com

Sanity & Self is dedicated to all women who want to have a better life.

See the terms and privacy policy for more information

Question? Contact us at support@sanityandself.com

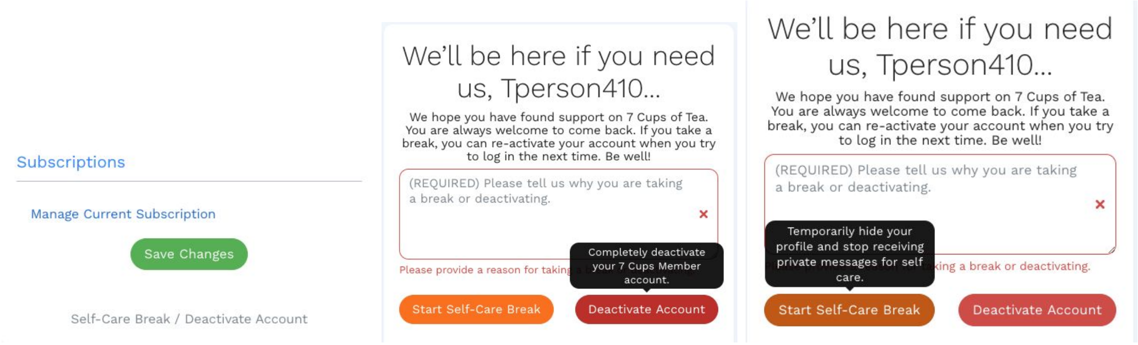
Are you sure that you want to delete your stored data? This may cause interuption to your service and will not end any active billing or subscription cycles.

```
Your data deletion request has been recieved and
your stored data will be completely deleted within
24 hours. If you continue to use Sanity & Self
Services, you will create new data.
```

*Figure 5: Sanity & Self's "Delete Data" process is outlined above*

For 2 of 7 apps, we did not find features and functionality present to delete information through the iOS app for 7 Cups and Talkspace. We found that using 7 Cups through the desktop interface (not the mobile interface) provides the possibility to allow the user to do 2 things:

- Start self-care break: Temporarily hide your profile and stop receiving private messages for self care
- Deactivate account: Completely deactivate your 7 Cups Member Account



We'll be here if you need us, Tperson410...

We hope you have found support on 7 Cups of Tea. You are always welcome to come back. If you take a break, you can re-activate your account when you try to log in the next time. Be well!

(REQUIRED) Please tell us why you are taking a break or deactivating.

Please provide a reason for taking

Completely deactivate your 7 Cups Member account.

We'll be here if you need us, Tperson410...

We hope you have found support on 7 Cups of Tea. You are always welcome to come back. If you take a break, you can re-activate your account when you try to log in the next time. Be well!

(REQUIRED) Please tell us why you are taking a break or deactivating.

Temporarily hide your profile and stop receiving private messages for self care.

king a break or deactivating.

*Figure 6: 7 Cups highlights there is a "Start Self-Care Break" and "Deactivate Account" option*

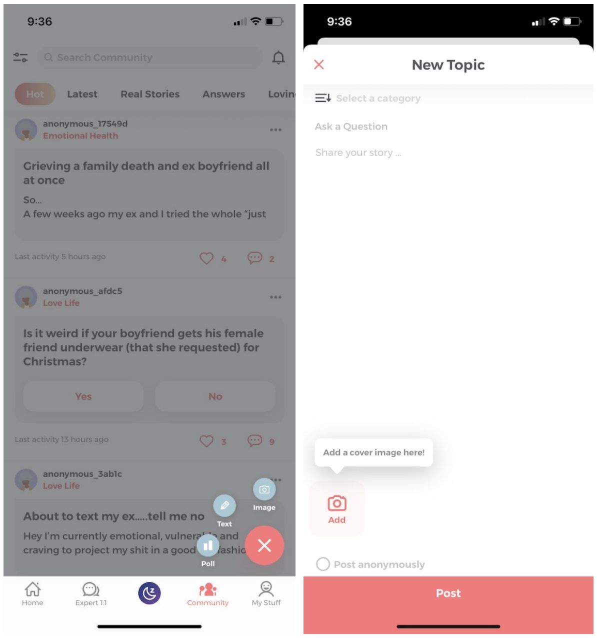
Looking at the language across all the apps, Youper makes it clear that account cancellation also deletes all user data. Wysa also offers a "reset my data" option in the settings page, which—based on their privacy policy terms—aligns with the "right to be forgotten" and is functionally equivalent to data deletion. The remaining 5 apps we evaluated did not make it clear whether doing something like deleting the account or deactivating the account or cancelling the account actually deletes the user's data.

### 4.2.4 - Companies may encourage mental health app users to share data in communities without clear disclosures in the app design and user interface that comments may be shared with the public.

People who are using a mental health app with a community feature should make it clear that the potentially sensitive mental health information may be shared to the public community using their platform. Companies need to be protecting data by default. For example, they should not be sharing this information with advertisers and it would be better to push data minimization or privacy by default over improved text disclosures. Sharing a comment or reply is a personal choice, but when someone is about to share or reply to a comment, it is not ideal to force someone to read a long body of text before engaging with the community.

2 of 7 apps have community forums as a core part of their app user experiences: Sanity & Self and 7 Cups. When the Sanity & Self user is about to share a post or reply to a post in the "community" forum, their profile (which may include an identifiable photo), their username (which may reflect personal information) or the sensitive text they reply about themselves in reference to the forum topic (on anxiety, depression, etc.) may be shared with many others on this forum. Users can delete their individual comments on threads. It is unclear whether deleting an account means all previous comments, likes, and replies are also automatically deleted. Similar to other

findings, this behavior is not necessarily unique to just the mental health apps explored here. However, we point this out since on these apps, people may be sharing information about anxiety, depression, or other potentially stigmatizing mental health issues.



anonymous_17549d
Emotional Health
Grieving a family death and ex boyfriend all at once
So...
A few weeks ago my ex and I tried the whole "just
Last activity 5 hours ago 4 2

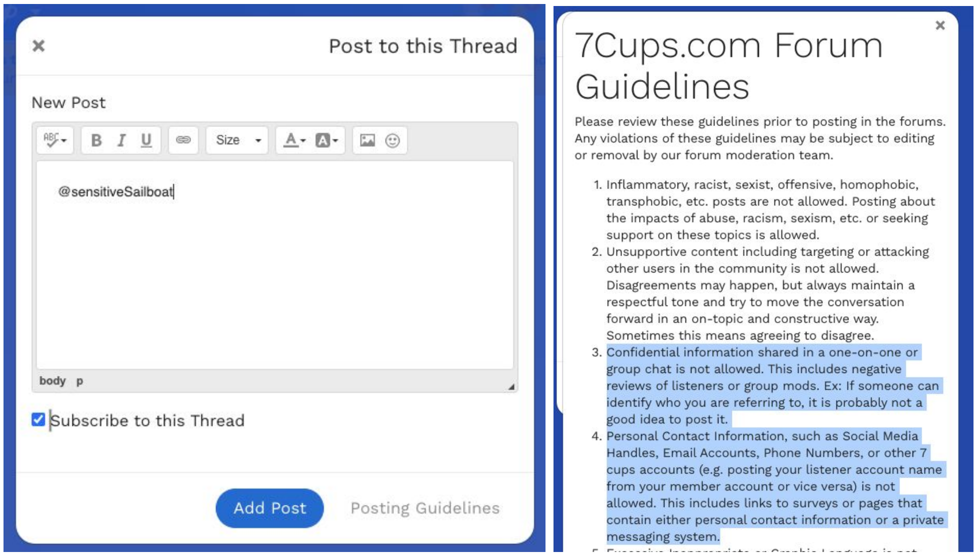
anonymous_afdc5
Love Life
Is it weird if your boyfriend gets his female friend underwear (that she requested) for Christmas?
Yes No
Last activity 13 hours ago 3 9

anonymous_3ab1c
Love Life
About to text my ex.....tell me no
Hey I'm currently emotional, vulnera[illegible] and craving to project my shit in a good [illegible]ashio

Ask a Question
Share your story ...

*Figure 7: Sanity & Self's screen captures that shows how a user may post a comment on the community forum feature*

We found that some apps such as LEGO, include safeguards for users like "nicknames" or anonymous username generators. This will ensure that a user (in this case, a child's) identity will not be shared through public community forums throughout the app. 7 Cups on the other hand, includes a passive, out-of-the-way option to highlight personal information guidelines. In the image on the left, there is a light gray link called "posting guidelines". If the user clicks on this, they can read the suggested posting guidelines (image right) around not posting confidential information where "someone can identify who you are referring to" and not posting "personal contact information such as social media handles, email accounts, phone numbers or other 8 cups accounts".



@sensitiveSailboat

☑ Subscribe to this Thread

7Cups.com Forum Guidelines

Please review these guidelines prior to posting in the forums. Any violations of these guidelines may be subject to editing or removal by our forum moderation team.

1. Inflammatory, racist, sexist, offensive, homophobic, transphobic, etc. posts are not allowed. Posting about the impacts of abuse, racism, sexism, etc. or seeking support on these topics is allowed.
2. Unsupportive content including targeting or attacking other users in the community is not allowed. Disagreements may happen, but always maintain a respectful tone and try to move the conversation forward in an on-topic and constructive way. Sometimes this means agreeing to disagree.
3. Confidential information shared in a one-on-one or group chat is not allowed. This includes negative reviews of listeners or group mods. Ex: If someone can identify who you are referring to, it is probably not a good idea to post it.
4. Personal Contact Information, such as Social Media Handles, Email Accounts, Phone Numbers, or other 7 cups accounts (e.g. posting your listener account name from your member account or vice versa) is not allowed. This includes links to surveys or pages that contain either personal contact information or a private messaging system.
5. Excessive Inappropriate or Graphic Language is not

*Figure 8: When posting to a thread on 7 Cups, a user has the option to see "Posting Guidelines" which highlights information around data sharing*

We do not suggest that companies burden people with consent models and a barrage of privacy information. We do not expect that users should read disclosures in the privacy policies. In fact, years of research[47] has documented that people will ignore these policies, especially upon onboarding. However, we highlight this as a common feature across many data-collecting apps that are consumer-facing.

[47] Auxier, Brooke, et al. "4. Americans' Attitudes and Experiences with Privacy Policies and Laws." Pew Research Center: Internet, Science &amp; Tech, Pew Research Center, 26 May 2020, www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/.

## Section 5. Recommendations

**Recommendation 1: Clearly explain procedures used for de-identification of data used for research. Identifiable data should not be shared except at the consumer's direction.**

We advocate for companies to improve clarity on research for data sharing especially around how they define “anonymized data.” Companies should be explicit about what processes they use to de-identify data. We highlight this to help prevent people from being reidentified. Mental health applications collect sensitive information that can create damaging, irreversible impacts on individuals if shared with third parties, including social stigmatization and additional barriers to future opportunities.

**Evidence:** In finding 4.2.1, we found that companies may opt users into research[48] by default or do it in a way that is not clearly outlined or articulated to the user.

MindDoc's privacy policy notes: “*MindDoc transmits your health data in a completely anonymous form to universities for research purposes.”* It is important to note that “completely anonymous” is not a clearly defined or or universally understood term. There has been years of documented research and experiments to show the nuance of claiming complete anonymization. In 2014, open data activists and researchers discovered[49] that New York taxi details (such as drivers' addresses and income) can be extracted from anonymized data. Researchers from Belgium's Université catholique de Louvain (UCLouvain) and Imperial College London “built a model to estimate how easy it would be to deanonymize any arbitrary dataset,” the Guardian reported.[50] Researchers have also created tools to prove that the average user has an “83 percent risk of re-identification,” reports[51] the Scientific American.

[48] Evan Selinger, Woodrow Hartzog. “Facebook's Emotional Contagion Study and the Ethical Problem of Co-Opted Identity in Mediated Environments Where Users Lack Control - Evan Selinger, Woodrow Hartzog, 2016.” SAGE Journals, journals.sagepub.com/doi/full/10.1177/1747016115579531.
[49] Vijay Pandurangan. “On Taxis and Rainbows” Medium, Vijay Pandurangan, 27 June 2014, tech.vijayp.ca/of-taxis-and-rainbows-f6bc289679a1.
[50] “'Anonymised' Data Can Never Be Totally Anonymous, Says Study.” The Guardian, Guardian News and Media, 23 July 2019, www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds.
[51] Bushwick, Sophie. "Anonymous" Data Won't Protect Your Identity. 23 July 2019, www.scientificamerican.com/article/anonymous-data-wont-protect-your-identity/.

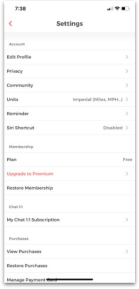
Sanity & Self’s privacy policy notes that the company “often conducts research on its customer demographics, interests and behavior [...] [and] may “share this aggregate data with its affiliates, agents and business partners” and “disclose aggregated user statistics in order to describe our services to current and prospective business partners, and to other third parties for other lawful purposes.” Here, there are not a lot of details about how they protect from reidentification.

According to Talkspace spokesperson John Kim, users cannot opt-out of research projects, but "All data used for research projects or to improve internal Talkspace therapist tools is de-identified data converted into "safe harbor" form using our own software which removes all personal "identifiers" at a level even higher than required by HIPAA protocols." In their privacy policy, Talkspace says, “We only provide data to our partners, if any, after we have removed your name and any other personally identifying information from it, or have combined it with other people's data in a way that it no longer personally identifies you.” This policy seems slightly more specific and provides good examples of deidentified usage, but still does not clearly explain how they process the data to reasonably ensure reidentification is not possible.

**Recommendation 2: Provide clear and contextually-appropriate explanations of how user-provided data will be used, so users are aware of potential consequences before they share.**

Companies should not overwhelm people with superfluous information or choices. Wherever possible, app default settings should be that your privacy is protected and users should not have to worry about managing this on their own. However, if there are choices to be made or information someone should be aware of, they should be presented in a clear and straightforward way.

**Evidence:**



7:38

Settings

Account

Edit Profile

Privacy

Community

Units Imperial (Miles, MPH...)

Reminder

Siri Shortcut Disabled

Membership

Plan Free

Upgrade to Premium

Restore Membership

Chat 1:1

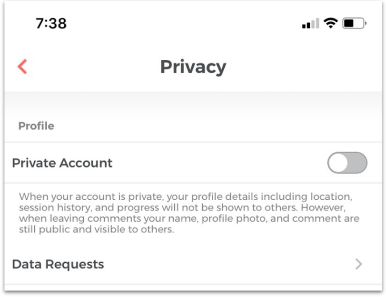
My Chat 1:1 Subscription

Purchases

View Purchases

Restore Purchases

Manage Payment Card



7:38

Privacy

Profile

Private Account

When your account is private, your profile details including location, session history, and progress will not be shown to others. However, when leaving comments your name, profile photo, and comment are still public and visible to others.

Data Requests

In Finding 4.2.2, we found that companies may design user profiles to be NOT private by default. Sanity and Self is a pattern of the broader ecosystem. We note that how potentially dangerous this is for a user may depend on the nature of the app, taking context (mental health data sensitivity) and the fact there is a social community built into the app. The default app functionality should be the most private and allow people to make their own decisions about what information is public.

In Finding 4.2.4, companies may encourage mental health app users to share data in communities without clear disclosures in the app design and user interface that comments may be shared with the public. If there is a community sharing feature, it should be clearer to the user what the implications are of engaging with people on sensitive mental health topics before they post on a public forum that may not be deletable or have consequences to their privacy. This should be presented in a digestible way in the user interface.

### Recommendation 3: Adhere to platform guidelines that are in place to protect people's privacy.

App developers should ensure that their apps meet the guidelines laid out in Android developer documentation, such as *Best Practices for Unique Identifiers* which recommends avoiding the use of identifiers like the Android ID (SSAID). App developers should also make sure that the libraries (SDKs) they embed within their apps meet their own expectations for data collection, and that they are configured accordingly.

**Evidence:** In Finding 4.1.1, we observed MindDoc and Sanity & Self transmit Android IDs and AAIDs within the same transmission to third party servers. We also observed Wysa transmit only Android IDs—not AAIDs—to two third-party servers.

### Recommendation 4: Transparently disclose the service providers that receive data when people use your apps.

We recommend that companies are more transparent in their privacy policies about the service providers that receive data. Although it is not legally required or common practice in the U.S. to list every service provider or institution receiving data, we recommend companies proactively disclose this information.

**Evidence:** In Finding 4.3, we found that only 4 of the 7 services made clear disclosures about with whom data are shared. Additionally, only 2 of the 7 services shared data in line with what they disclosed in their policies.

## Section 6. Conclusion

Mental health apps show many of the same patterns we see elsewhere in data-collecting apps. However, the sensitivity of the data they collect means the privacy practices and policies are even more important—especially during a pandemic where people are relying on these services in greater numbers for the first time. Our evaluation shows how there are multiple ways to evaluate how thoughtfully mental health apps handle user data collection, management, and sharing to third parties.

We call for all apps to improve on the recommendations highlighted in Section 5—adhere to platform guidelines, institute clear explanations of de-identification of data used for research, increase privacy awareness in the main user experience and be transparent about the service providers that receive user data. Some apps may outwardly mention the third party companies they share in their privacy policies while others may not mention any. Some apps may create clear ways to delete one's data through the mobile app, while others may limit this user right to California residents based on CCPA. Some apps over collect data such as geolocation which is not necessarily for the app to function. Consumer Reports recognizes there are many nuanced design and data governance decisions that factor into offering high-quality and private-by-design service. By comparatively evaluating popular apps, we can clarify how companies can continue to raise the standard in this emerging category, ensure that consumers consent to the collection and sharing of sensitive mental health data, and ensure that consumers can trust in these services to be good stewards of their data.