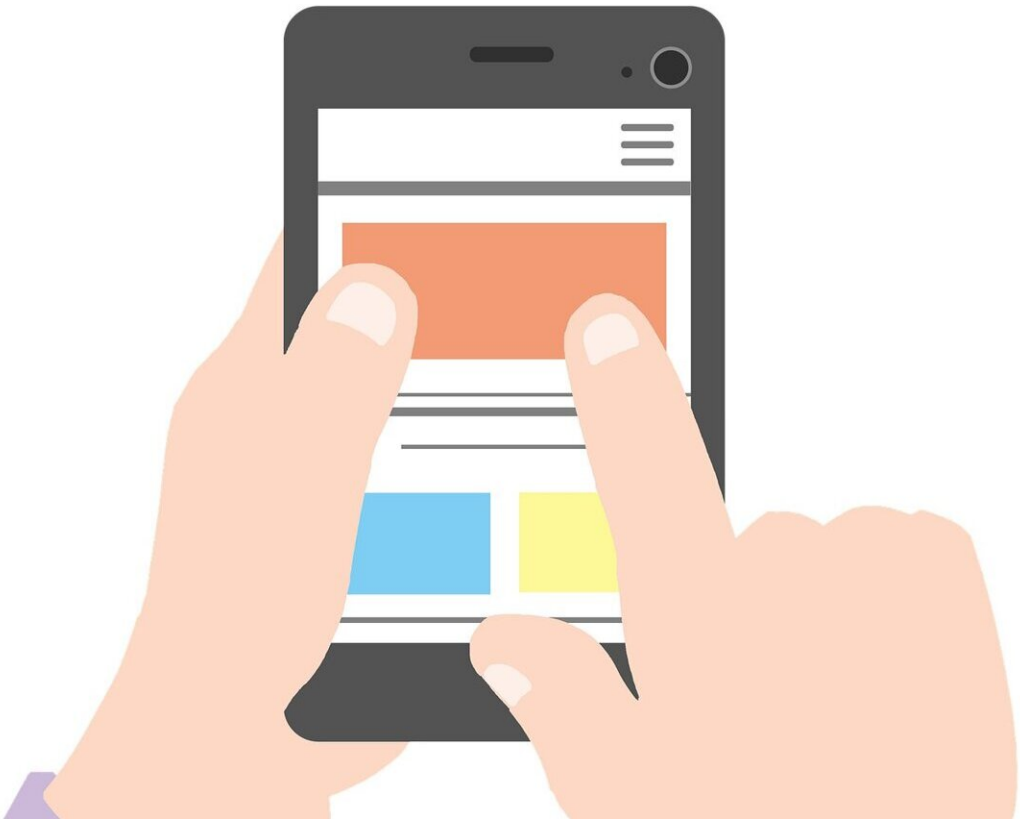
Mental health apps may put your privacy at risk. Here's what to look for

May 3 2023, by Jon Healey



Credit: Pixabay/CC0 Public Domain

Every second, thousands of people tell their phone or computer something about themselves that they might not want anyone else to know.

That's what happens when people search for medical information online, typically looking for answers to questions about a problem or worry they have. In 2022, Google says, its users searched often for information about diets and supplements, exercise, stress and depression, and various other ailments. Depending on the users' browser settings, those details may still be found in their Google profiles.

And internet searches are just one of many ways people share sensitive personal health data.

They're also doing so on health and wellness apps, including mental health and counseling programs. These apps collect data about their users to provide services—and, in many cases, to generate revenue, whether it be through targeted advertisements or sales of anonymized information to data brokers.

On Tuesday, researchers at Mozilla released their latest report on the privacy practices of popular mental health apps, finding that almost 60% fell short of the company's minimum standards. In fact, Mozilla said, 40% of the apps reviewed had worse privacy practices this year than they did last year.

California law helps residents protect themselves against apps' bad data practices, but they still have to be proactive. Jen Caltrider, director of Mozilla's Privacy Not Included work, said it's important to read an app's privacy policy before downloading it, because some of them start collecting data from users moments after they're activated.

Privacy not included

Researchers have been pointing out problems in health data privacy for years. One reason is that the data has value, even when the user's name is not attached to it; advertisers can still use anonymized information to

send targeted ads to people based on their health concerns and afflictions.

Another reason is that the federal law protecting personal health data doesn't reach many of the companies collecting and sharing the data. Instead, the Health Information Portability and Accountability Act applies only to doctors, hospitals and the companies they have business agreements with.

That's why Facebook can collect "details about patients' doctor's appointments, prescriptions, and health conditions on hospital websites," according to the Markup, and Google can store data on the days you went to see your doctor (or your psychiatrist). And it's why mental health apps routinely collect and share personal information about their users. According to a study of 578 mental health apps published in December in the Journal of the American Medical Assn., 44% shared data they collected with third parties.

Mozilla looked at 32 mental health apps a year ago that offered such services as direct input from therapists online, community support pages, well-being assessments and AI chat bots. Caltrider's team examined what data the apps were collecting, what they told users they were doing with their personal information, whether users could change or delete the information collected, how solid their basic security practices were, and what the developers' track records were.

Twenty-nine of the apps—90% of those studied—didn't meet Mozilla's minimum standards when it released its report last May, earning a Privacy Not Included warning label on Mozilla's site. "Despite these apps dealing with incredibly sensitive issues—like depression, anxiety, suicidal thoughts, domestic violence, eating disorders, and [post-traumatic stress disorder]—the worst of them routinely share data, target vulnerable users with personalized ads, allow weak passwords, and

feature vague and poorly written privacy policies," the company said.

Since then, the company said, six of the reviewed apps have improved on the privacy and security front. In some cases, such as with the Modern Health app, they simply made clear in their privacy policies that they were not, in fact, selling or disclosing personal information to third parties. In others, such as with Youper and Woebot, the apps made their privacy and password policies significantly stronger.

But 10 other apps went in the other direction, Mozilla said, weakening their privacy or security policies, or both. All told, almost 60% of the apps reviewed earned Mozilla's warning label, including Sesame Workshop's Breathe, Think, Do app for children, which Caltrider said doesn't appear to collect much personal information, but which has a troublingly permissive privacy policy.

Only two apps—PTSD Coach (offered by the U.S. Department of Veterans Affairs) and the Wysa AI chatbot—were recommended for their handling of personal data. The same two apps topped Mozilla's list last year too, although Mozilla's researchers acknowledged that they didn't know if Wysa's AI "has enough transparency to say they avoid racial, gender or cultural bias."

For details on the apps reviewed, consult the chart Mozilla posted on its site showing which problems were identified. For example, Talkspace and BetterHelp "pushed consumers into taking questionnaires up front without asking for consent or showing their privacy policies," then used the information for advertising, Mozilla said. The company also found that Cerebral made "799 points of contact with different ad platforms during one minute of app activity."

Why data privacy matters

Although Americans are starting to talk more openly about their mental health, Caltrider said, "it's something that a lot of people want to keep private or close to the vest."

That's not just because of the lingering stigma attached to some mental health issues. It's also because of the real risk of harm that people face if their personal information gets shared for the wrong reasons.

For instance, Caltrider said, you might tell a mental health app that you're seeing a therapist three times a week for obsessive-compulsive disorder or that you have an eating disorder. Now imagine that information finding its way into the anonymous profile advertisers have assigned to you—do you want those ads showing up in your browser, especially when you're at work? Or in your email?

It doesn't take much imagination, actually. Data brokers are, in fact, collecting and selling mental health data, according to a report released last month by Duke University.

"The 10 most engaged brokers advertised highly sensitive mental health data on Americans, including data on those with depression, attention disorder, insomnia, anxiety, ADHD, and bipolar disorder as well as data on ethnicity, age, gender, zip code, religion, children in the home, marital status, net worth, credit score, date of birth, and single parent status," the report states. "Whether this data will be deidentified or aggregated is also often unclear, and many of the studied data brokers at least seem to imply that they have the capabilities to provide identifiable data."

Nor did many of the brokers have meaningful controls on whom they sold the data to or how the information could be used, the report said.

Political disinformation campaigns have targeted people whose profiles

include specific characteristics related to mental health, such as depression, Caltrider said. In addition, she said, health insurers buy information from data brokers that could affect the premiums charged in communities with higher instances of mental health issues.

Companies using their knowledge of your mental-health issues to target you with advertising, or enable other companies to target you, "kind of gets sick and creepy," Caltrider said.

Many app developers will insist that they don't share personally identifiable information, but studies have shown that supposedly anonymous profiles can be linked to real names and attributes if they contain enough scraps of detail (especially if the scraps include location data). "Users must really trust that the company takes the best measures possible to make sure all this data is actually truly anonymized and de-identified," Mozilla's researchers warned.

What you can do

The California Consumer Privacy Act and the ballot measure that strengthened it, the California Privacy Rights Act, require businesses operating in the state to reveal what personal information they collect about you and let you limits its use, forbid its sale to third parties, correct errors and even delete it. Notably, the laws do not apply to data that cannot reasonably be associated with a specific person, which means that businesses can share personal information that's anonymized.

That's why privacy advocates urge you to take steps that will prevent your data from being collected and shared by mental health apps. These include:

—Read the privacy policy. Yes, they're often dense and legalistic, but Caltrider pointed to several potential flags that you can look for: Does

the company sell data? Does it give itself permission to widely share the data it collects? Does it acknowledge your right to to access and delete your data?

One other benefit of the state's privacy laws is that many websites now offer within their privacy policies a statement of California users' rights. Caltrider said this version has to spell out clearly how the company plans to use your data, so it's easier to digest than the typical privacy policy.

What about apps that don't have a privacy policy? "Never download those apps," Caltrider said.

There is no federal law on data privacy, but the Federal Trade Commission uses its authority to crack down on companies that do not truthfully disclose what they do with your data. See, for example, the settlement it reached last year with Flo Health, the maker of a fertility-tracking app that allegedly shared personal data about its users despite promising not to do so in its privacy policy.

—Skip apps that are no longer supported.If there's no one monitoring an app for bugs and security holes, Caltrider said, hackers could find and then share techniques for using the app as a gateway into your phone and the information you store there. "It could leave you really vulnerable," she said.

Granted, it may be hard to tell an app that's been abandoned by its developer from one that hasn't. Caltrider suggested checking the app information page in the Apple App or Google Play store to see when it was last updated; if it's been two to four years since the last update, that may be a sign that it is no longer supported.

—Don't rely on the privacy information in the app store. In the description provided for each app, Google and Apple offer summaries

of the data collected and shared. But Caltrider said that the information is supplied by the app developers themselves, not an independent source. And in Google's case, she said, the information was riddled with errors.

On the plus side, the Google Play store allows you to see what permissions the app wants before you download it—click on the "About this app" link in the app description, then scroll to find the "See More" link under "App permissions." Does the app want access to your photos, your location or your phone's stored files? Does it want permission to place a unique ID for targeted advertisements? All of these permissions have implications for your privacy, and they all tell you something about the app's business model.

You can't check permissions prior to downloading apps from Apple's App store. Instead, if you want to check an app's permissions, go to Settings on your iPhone, select "Privacy & Security," then select "App Privacy Report." You can then go back to the Privacy & Security section to delete permissions one at a time, if you wish.

—Don't use your Facebook or Google ID to sign into an app.Linking your app to these companies invites them to collect more data about your life online, which feeds their ad-targeting economies.

—Use video instead of text where possible. The mental health counseling offered via chatbots, AI apps and other nonprofessional care providers isn't covered by HIPAA, so any transcripts won't be protected by federal law. What you disclose to those apps in writing could exist forever in unencrypted form, Caltrider said, and you may have no way of knowing who can see it or what it's being used for. "I would do video-based conversations that aren't going to be recorded," she said.