NEWS

Privacy concerns about mental health apps highlight need for regulation

BY **PETER HESS**

6 NOVEMBER 2019

Apps spell big business in the healthcare industry: Dozens of apps are marketed to people with conditions including depression, anxiety and autism. And Google parent company Alphabet announced Friday that it will buy **wearable fitness tracker company FitBit**.

But many app developers sell users' data, including their name, medical status and sex, to third parties such as Facebook and Google, researchers warn. And most consumers are unaware that their data can be used against them.

For instance, the U.S. **government has investigated Facebook** for allowing housing ads to filter out individuals based on several categories protected under the Fair Housing Act, including disability status.

"There can also be usages to exclude certain populations, including people living with autism, from benefits like insurance," says **Nir Eyal**, professor of bioethics at Rutgers University in New Jersey.

Eyal and others say that the extensive personal information apps can gather from users may help researchers tailor treatments, but these benefits should not come at the expense of the users' privacy.

Ultimately, some researchers say, the government may need to get involved in regulating this fast-moving marketplace — "the same way we force cigarette companies to put a big warning," says **Guillermo Sapiro**, professor of electrical and computer engineering at Duke University in North Carolina.

Shopping for apps:

Many researchers are increasingly exploring the use of apps in screening for and treatment of autism. Most screening apps are still **not ready** for **clinical use**, but once validated, they promise to provide objective measures of autism traits using machine learning, minimizing the subjective bias clinicians can bring to the process.

Apps also enable researchers to recruit larger pools of study participants than they might be able to recruit locally. And they can expand the reach of healthcare options for individuals and families who don't have reliable access to professional care near their home.

For these research purposes, standards set by the government and by institutional review boards typically ensure that the data collected is secure. However, developers of commercial apps are frequently not transparent about how a user's health data will be collected, stored and used.

A study published in March in *The BMJ* showed that 19 of 24 of the most popular health apps in the Google Play marketplace transmitted user data to at least one third-party recipient[1]. An app called **Medsmart Meds & Pill Reminder**, for example, sent user data to four different companies.

Another study, published in April in *JAMA Network Open*, found that 33 of 36 top-ranked depression and smoking cessation apps the investigators looked at sent user data to a third party[2]. Of them, 29 shared the data with Google, Facebook or both, and 12 of those did not disclose that use to the consumer.

Moodpath, the most popular app for depression on Apple’s app store, shares user data with Facebook and Google. The app’s developer discloses this fact, but the disclosures are buried in the seventh section of the app’s **privacy policy**. Facebook also **buys and sells user data** to better target advertising to specific users, and does so even with users who don’t have a Facebook account.

Even when apps disclose their policies, the risks involved are not always clear to consumers, says **John Torous**, director of digital psychiatry at Beth Israel Deaconess Medical Center in Massachusetts and co-lead investigator on the April study. “It is clear that most privacy policies are nearly impossible to read and understand,” Torous says.

Digital prescriptions:

For these reasons, some experts say, most apps should not be marketed directly to consumers without a healthcare professional’s recommendation.

What’s more, the benefits of **so few apps are supported** by direct evidence that almost none can be recommended to consumers, Sapiro says.

Sapiro says app developers can collect data, but they owe it to their users to be transparent about what data are being collected and how the information will be used. If the data will be shared with a third party but that disclosure “is buried in the 75 pages of consent,” he says, “I would call it dishonesty from the provider.”

Sapiro’s team has been working on a screening app called Autism & Beyond, which uses **Apple’s open-source ResearchKit tool**. The data is stored securely on Duke Health System’s servers. The researchers use cloud computing for their machine-learning algorithms, allowing them to query the data detached from any personally identifiable information.

They are also fully transparent with participants about this process. When participants download the app, they see a few important highlights at the beginning of the informed consent agreement. And at the end, Sapiro says, “we [give] a very small test to the user to see if they really understood the consent.”

?Still, even this approach may not be enough, says Torous.

“I have seen some quizzes for online privacy policies that one can just click through, so getting the questions correct does not always mean the person has been well informed,” Torous says.

He applauds **the apps** used by the U.S. Department of Veterans Affairs, which he says communicate privacy issues in simple and plain language. “These don’t always need to be long and complex,” he says.

The Molehill Mountain app, an anxiety app for autistic people developed by the U.K.-based charity Autistica, also features a plain-language **privacy statement**. It prominently states exactly what information the app will collect from users, how the developers will use those data and what users’ rights are concerning their own data.

REFERENCES:

1. Grundy Q. *et al. BMJ* **364**, 1920 (2019) **PubMed**
2. Huckvale K. *et al*. *JAMA Netw. Open* **2**, e192542 (2019) **PubMed**