

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.

<https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636>

# You Give Apps Sensitive Personal Information. Then They Tell Facebook.

Wall Street Journal testing reveals how the social-media giant collects a wide range of private data from developers; 'This is a big mess'

*By Sam Schechner and Mark Secada*

Feb. 22, 2019 11:07 a.m. ET

Millions of smartphone users confess their most intimate secrets to apps, including when they want to work on their belly fat or the price of the house they checked out last weekend. Other apps know users' body weight, blood pressure, menstrual cycles or pregnancy status.

Unbeknown to most people, in many cases that data is being shared with someone else:

Facebook Inc. [FB 1.16% ▲](#)

The social-media giant collects intensely personal information from many popular smartphone apps just seconds after users enter it, even if the user has no connection to Facebook, according to testing done by The Wall Street Journal. The apps often send the data without any prominent or specific disclosure, the testing showed.

It is already known that many smartphone apps send information to Facebook about when users open them, and sometimes what they do inside. Previously unreported is how at least 11 popular apps, totaling tens of millions of downloads, have also been sharing sensitive data entered by users. The findings alarmed some privacy experts who reviewed the Journal's testing.

Facebook is under scrutiny from Washington and European regulators for how it treats the information of users and nonusers alike. It has been fined for allowing now defunct political-data firm Cambridge Analytica illicit access to users' data and has drawn criticism for giving companies special access to user records well after it said it had walled off that information.

In the case of apps, the Journal's testing showed that Facebook software collects data from many apps even if no Facebook account is used to log in and if the end user isn't a Facebook

member.

Apple Inc. and Alphabet Inc.'s Google, which operate the two dominant app stores, don't require apps to disclose all the partners with whom data is shared. Users can decide not to grant permission for an app to access certain types of information, such as their contacts or locations. But these permissions generally don't apply to the information users supply directly to apps, which is sometimes the most personal.

In the Journal's testing, Instant Heart Rate: HR Monitor, the most popular heart-rate app on Apple's iOS, made by California-based Azumio Inc., sent a user's heart rate to Facebook immediately after it was recorded.

Flo Health Inc.'s Flo Period & Ovulation Tracker, which claims 25 million active users, told Facebook when a user was having her period or informed the app of an intention to get pregnant, the tests showed.

Real-estate app Realtor.com, owned by Move Inc., a subsidiary of Wall Street Journal parent News Corp, sent the social network the location and price of listings that a user viewed, noting which ones were marked as favorites, the tests showed.

None of those apps provided users any apparent way to stop that information from being sent to Facebook.

Facebook said some of the data sharing uncovered by the Journal's testing appeared to violate its business terms, which instruct app developers not to send it "health, financial information or other categories of sensitive information." Facebook said it is telling apps flagged by the Journal to stop sending information its users might regard as sensitive. The company said it may take additional action if the apps don't comply.

"We require app developers to be clear with their users about the information they are sharing with us," a Facebook spokeswoman said.

At the heart of the issue is an analytics tool Facebook offers developers, which allows them to see statistics about their users' activities—and to target those users with Facebook ads. Although Facebook's terms give it latitude to use the data uncovered by the Journal for other purposes, the spokeswoman said it doesn't do so.

Facebook tells its business partners it uses customer data collected from apps to personalize ads and content on Facebook and to conduct market research, among other things. A patent the company applied for in 2015, which was approved last year, describes how data from apps would be stored on Facebook servers where it could be used to help the company's algorithms target ads and select content to show users.

Apple said its guidelines require apps to seek “prior user consent” for collecting user data and take steps to prevent unauthorized access by third parties. “When we hear of any developer violating these strict privacy terms and guidelines, we quickly investigate and, if necessary, take immediate action,” the company said.

A Google spokesman declined to comment beyond pointing to the company’s policy requiring apps that handle sensitive data to “disclose the type of parties to which any personal or sensitive user data is shared,” and in some cases to do so prominently.

Before Alice Berg began using Flo to track her periods last June, she checked the app’s terms of service. The 25-year-old student in Oslo says she had grown more cautious about sharing data with apps and wanted to ensure that only a limited amount of her data would be shared with third-parties like Facebook.

Now Ms. Berg said she may delete the app. “I think it’s incredibly dishonest of them that they’re just lying to their users especially when it comes to something so sensitive,” she said.

Flo Health’s privacy policy says it won’t send “information regarding your marked cycles, pregnancy, symptoms, notes and other information that is entered by you and that you do not elect to share” to third-party vendors.

Flo initially said in a written statement that it doesn’t send “critical user data” and that the data it does send Facebook is “depersonalized” to keep it private and secure.

The Journal’s testing, however, showed sensitive information was sent with a unique advertising identifier that can be matched to a device or profile. A Flo spokeswoman subsequently said the company will “substantially limit” its use of external analytics systems while it conducts a privacy audit.

Move, the owner of real-estate app Realtor.com—which sent information to Facebook about properties that users liked, according to the Journal’s tests—said “we strictly adhere to all local, state and federal requirements,” and that its privacy policy “clearly states how user information is collected and shared.” The policy says the app collects a variety of information, including content in which users are interested, and may share it with third parties. It doesn’t mention Facebook.

The Journal tested more than 70 apps that are among the most popular in Apple’s iOS store in categories that handle sensitive user information. The Journal used software to monitor the internet communications triggered by using an app, including the information being sent to Facebook and other third parties. The tests found at least 11 apps sent Facebook potentially sensitive information about how users behaved or actual data they entered.



Apple Chief Executive Tim Cook condemned what he described as a 'data-industrial complex' in an October speech to privacy regulators in Europe. PHOTO: STEPHANIE LECOCQ/EPA/SHUTTERSTOCK

Among the top 10 finance apps in Apple's U.S. app store as of Thursday, none appeared to send sensitive information to Facebook, and only two sent any information at all. But at least six of the top 15 health and fitness apps in that store sent potentially sensitive information immediately after it was collected.

Disconnect Inc., a software company that makes tools for people to manage their online privacy, was commissioned by the Journal to retest some of the apps. The company confirmed the Journal's findings, and said Facebook's terms allowing it to use the data it collected were unusual.

"This is a big mess," said Patrick Jackson, Disconnect's chief technology officer, who analyzed apps on behalf of the Journal. "This is completely independent of the functionality of the app."

The software the Journal used in its tests wasn't able to decipher the contents of traffic from Android apps. Esther Onfroy, co-founder of cybersecurity firm Defensive Lab Agency, conducted a separate test showing that at least one app flagged by the Journal's testing, BetterMe: Weight Loss Workouts, was in its Android version also sharing users' weights and heights with Facebook as soon as they were entered.

BetterMe Ltd. didn't respond to email and social-media inquiries from the Journal. On Feb. 16, after being contacted by the Journal, it updated its privacy policy, replacing a general reference to Facebook's analytics to one that says it shares information with Facebook so it can determine "the average weight and height of our users, how many users chose a particular problem area of their body, and other interactions."

Apps often integrate code known as software-development kits, or SDKs, that help developers integrate certain features or functions. Any information shared with an app may also be shared

with the maker of the embedded SDK. There are an array of SDKs, including Facebook's, that allow apps to better understand their users' behavior or to collect data to sell targeted advertising.

Such data-sharing among apps through the use of SDKs is "industry standard practice," a Facebook spokeswoman said.

Facebook's SDK, which is contained in thousands of apps, includes an analytics service called "App Events" that allows developers to look at trends among their users. Apps can tell the SDK to record a set of standardized actions taken by users, such as when a user completes a purchase. App developers also can define "custom app events" for Facebook to capture—and that is how the sensitive information the Journal detected was sent.

Facebook says on its website it uses customer data from its SDK, combined with other data it collects, to personalize ads and content, as well as to "improve other experiences on Facebook, including News Feed and Search content ranking capabilities."

But the spokeswoman said Facebook doesn't use custom events—the ones that can contain sensitive information—for those purposes. She said Facebook automatically deletes some sensitive data it might receive, such as Social Security numbers.

She said Facebook is now looking into how to search for apps that violate its terms, and to build safeguards to prevent Facebook from storing sensitive data that apps may send.

Privacy lawyers say the collection of health data by nonhealth entities is legal in most U.S. states, provided there is sufficient disclosure in an app's and Facebook's terms of service. The Federal Trade Commission has taken an interest in cases in which data sharing deviates widely from what users might expect, particularly if any explanation was hard for users to find, said Woodrow Hartzog, a professor of law and computer science at Northeastern University.

The privacy policy for Azumio, maker of the Instant Heart Rate app, says it collects health information including heart rates, and that it may provide some personal data to third-party service providers and advertising providers. It doesn't say anything about providing those outside entities with health information drawn from its apps, nor does it mention Facebook as a provider.

Bojan Bostjancic, the company's CEO, said in an email message that it uses Facebook analytics to analyze its users' behavior in the app, and that it discloses the use of third parties in its privacy policy. He didn't respond to follow-up questions.

After being contacted by the Journal, Breathe Inc., maker of a meditation app of the same name, stopped sending Facebook the email address each user used to log in to the app, as well as the

full name of each meditation completed.

“Clearly, Facebook’s business model is unique and, unfortunately, we were not as diligent in aligning our data management with their privacy policy as we should have been,” said Garner Bornstein, the company’s co-founder.

In the European Union, the processing of some sensitive data, such as health or sexual information, is more tightly regulated. The EU’s new privacy law usually requires companies to secure explicit consent to collect, process or share such data—and making consent a condition of using a service usually isn’t valid.

Some privacy experts who reviewed the Journal’s findings said the practices may be in violation of that law. “For the sensitive data, companies basically always need consent—likely both the app developer and Facebook,” said Frederik J. Zuiderveen Borgesius, a law professor at Radboud University in the Netherlands.

The Facebook spokeswoman said the company is in compliance with the EU privacy law.



A Las Vegas monorail with a Google advertisement passes an Apple billboard about privacy. PHOTO: ROBYN BECK/AGENCE FRANCE-PRESSE/GETTY IMAGES

Facebook allows users to turn off the company’s ability to use the data it collects from third-party apps and websites for targeted ads. There is currently no way to stop the company from collecting the information in the first place, or using it for other purposes, such as detecting fake accounts. Germany’s top antitrust enforcer earlier this month ordered Facebook to stop using that data at all without permission, a ruling Facebook is appealing.

Under pressure over its data collection, Facebook Chief Executive Mark Zuckerberg said last year that the company would create a feature called “Clear History” to allow users to see what data Facebook had collected about them from applications and websites, and to delete it from

Facebook. The company says it is still building the technology needed to make the feature possible.

Data drawn from mobile apps can be valuable. Advertising buyers say that because of Facebook's insights into users' behavior, it can offer marketers better return on their investment than most other companies when they seek users who are, say, exercise enthusiasts, or in the market for a new sports car. Such ads fetch a higher cost per click.

That is partly why Facebook's revenue is soaring. Research firm eMarketer projects that Facebook this year will account for 20% of the \$333 billion world-wide digital-advertising market.

In a call to discuss the company's most recent earnings, however, Chief Financial Officer David Wehner noted that investors should be aware that Apple and Google could possibly tighten their privacy controls around apps. That possibility, he said, is "an ongoing risk that we're monitoring for 2019."

—*Mark Secada, Yoree Koh and Kirsten Grind contributed to this article.*

**Write to Sam Schechner at [sam.schechner@wsj.com](mailto:sam.schechner@wsj.com)**

*Appeared in the February 23, 2019, print edition as 'Apps Send User Secrets to Facebook.'*

Copyright © 2019 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.