1923133

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: / L Q.DK D Q & K D L U . K D Q m] bp$K ÎQå P4E,p$ bp$ ' TÀ °ÎWD Q

In the Matter of FLO HEALTH, INC.	DOCKET NO. &

COMPLAINT

The Federal Trade Commission ("FTC"), having reason to believe that Flo Health, Inc., a corporation ("Respondent"), has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Flo Health, Inc. ("Flo Health") is a Delaware corporation with its principal office or place of business at 1013 Centre Road, Suite 403-B, Wilmington, Delaware 19805.

2. Respondent has developed, advertised, offered for sale, sold, and distributed the Flo Period & Ovulation Tracker, a mobile application ("app") powered by artificial intelligence that functions as an ovulation calendar, period tracker, and pregnancy guide ("Flo App").

3. Millions of women use the Flo App, giving Respondent details of their menstruations and gynecological health on the promise that the app will help predict ovulation and aid in pregnancy and childbirth. These users trust Respondent with intimate details of their reproductive health because Respondent repeatedly promised to protect the information and keep it secret. Indeed, Respondent's privacy policies stated, time and again, that Respondent would not share users' health details with anyone.

4. In fact, beginning in 2016, Respondent handed users' health information out to numerous third parties, including Google, LLC ("Google"); Google's separate marketing service, Fabric ("Fabric"); Facebook, Inc. through its Facebook Analytics tool ("Facebook"); marketing firm AppsFlyer, Inc. ("AppsFlyer"); and analytics firm Flurry, Inc. ("Flurry"). And Respondent took no action to limit what these companies could do with the users' information. Rather, they merely agreed to each company's standard terms of service. By doing so, Respondent gave these third parties the ability to use Flo App users' personal health information expansively, including for advertising.

5. Respondent shared women's personal health information with these third parties for years, while at the same time promising them privacy. It was not until February 2019, when the Wall Street Journal revealed the practice, that Respondent halted sharing the data. Indeed, Respondent stopped sharing users' health information with Facebook the day after the exposé.

6. Upon learning that Respondent had turned some data related to their menstruations, pregnancies, and childbirths over to these third parties, hundreds of users wrote to Respondent, stating that they were "outraged," "incredibly upset," "disturbed," "appalled," and "very angry." Indeed, they felt "victimized" and "violated" by Respondent's actions.

7. The acts and practices of Respondent alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

Flo App

8. Since at least 2016, Respondent has made the Flo App available to users for free download from the Apple App Store and the Google Play Store. In the product description available on the Apple App Store, Respondent describes the Flo App as "a smart and simple period tracker, helpful pregnancy week by week app, accurate ovulation and fertility calendar and PMS symptoms tracker for women all over the world."

9. The Flo App is one of the most popular health and fitness apps available to consumers. Since 2016, more than 100 million users have downloaded the Flo App, including more than 16 million users across the United States and more than 19 million users in the European Union ("EU") and Switzerland. In 2019, the Flo App was the most downloaded health and fitness app in the Apple App store, and was the "App of the Day" in the Apple App Store in over 30 countries.

10. During the relevant time period, Respondent contracted with dozens of third-party firms to provide, among other things, various marketing and analytics services in connection with the Flo App. These firms included Facebook's analytics division, Google's analytics division, Fabric, AppsFlyer, and Flurry. Respondent did not contractually limit how these third parties could use data they received from the Flo App. In fact, the Terms of Service governing the agreements permitted the third parties to use the data for their own purposes.

11. Respondent encourages women to input vast quantities of health information into the Flo App: "Log your menstruation days in a handy period calendar, ovulation and fertility tracker, schedule menstrual cycle reminders, record moods and PMS symptoms, use a due date calculator, follow a pregnancy calendar ...." By doing so, Respondent tells users, you can "take full control of your health."

12. By encouraging millions of women to input extensive information about their bodies and mental and physical health, Respondent has collected personal information about consumers, including name, email address, date of birth, place of residence, dates of menstrual cycles, when pregnancies started and ended, menstrual and pregnancy-related symptoms, weight, and temperature.

Respondent’s

For Years, Respondent Disclosed Health Data About Millions of App Users to Facebook, Google, and Other Third Parties

18. Like most app developers, Respondent tracks "Standard App Events," records of routine app functions, such as launching or closing the app, as well as "Custom Apps Events," records of user-app interactions unique to the Flo App. For example, when a user enters menstruation dates, Respondent records the user's interaction with that feature as a Custom App Event. Respondent analyzes Custom App Events to improve the Flo App's functionality and identify which features are likely to interest new users.

19. Respondent gave each Custom App Event a descriptive title. For example, when a user enters the week of her pregnancy, Respondent records the Custom App Event "R_PREGNANCY_WEEK_CHOSEN." When a user selects a feature to receive menstruation reminders in the "wanting to get pregnant branch" of the app, Respondent records the Custom App Event "P_ACCEPT_PUSHES_PERIOD." Consequently, many of Respondent's Custom App Events convey information about users' menstruation, fertility, or pregnancies.

20. Despite its repeated representations between 2017 and 2019 that it would keep users' health data secret, Respondent disclosed health information to various third parties. In fact, as far back as June 2016, Respondent integrated into the Flo App software development tools, known as software development kits ("SDKs"), from the numerous third-party marketing and analytics firms mentioned above, including Facebook, Flurry, Fabric, AppsFlyer, and Google. These SDKs gathered the unique advertising or device identifiers and Custom App Events of the millions of Flo App users. By including sensitive health information in the titles of the Custom App Events, Respondent conveyed the health information of millions of users to these third parties for years. This directly contradicted Respondent's statements in its privacy policies that it would not divulge such information. Specifically, Respondent disclosed Custom App Event information to:

A. Facebook from June 2016 to February 2019;

B. Flurry from June 2016 to February 2019;

C. Fabric from November 2016 to February 2019;

D. AppsFlyer from May 2018 to February 2019; and

B. “This is private personal data and I feel disgusted that you are now making this data available to third parties.”

C. “Why would you EVER think it is ok to share that personal, private information with a third [sic] party?”

26. More than 100 Flo App users asked Respondent to delete their accounts and/or data or told the company they were deleting, or would delete, the Flo App.

Respondent’s

32. To join the EU-U.S. and/or Swiss-U.S. Privacy Shield Framework, a company must self-certify to Commerce that it complies with the Privacy Shield Principles, and to related requirements that have been deemed to meet the European Union's Adequacy Standard. Participating companies must annually re-certify their compliance.

33. The Privacy Shield expressly provides that, while decisions by organizations to "enter the Privacy Shield are entirely voluntary, effective compliance is compulsory: organizations that self-certify to the Department and publicly declare their commitment to adhere to the Principles **must comply fully** with the Principles." (emphasis added).

34. Companies under the jurisdiction of the FTC are eligible to join the EU-U.S. and/or Swiss-U.S. Privacy Shield Framework. Both frameworks warn companies that claim to have self-certified to the Privacy Shield Principles that failure to comply or otherwise to "fully implement" the Privacy Shield Principles "is enforceable under Section 5 of the Federal Trade Commission Act."

Respondent's Failure to Provide Adequate Notice for Third-Party Use of Health Information for Advertising and Other Purposes

35. Privacy Shield Principle 1, "Notice," requires organizations to inform individuals about, among other things, "the type or identity of third parties to which it discloses personal information, and the purposes for which it does so." Principle 1(a)(vi). It provides further: "This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party." Principle 1(b).

36. Respondent did not provide notice in clear and conspicuous language about the purposes for which it disclosed health information to third parties. When users in the European Union, Switzerland, Norway, Lichtenstein, and Iceland opened the Flo App for the first time, they were greeted by a "Welcome" screen that provided that by using the Flo App, the user consented to Respondent's aforementioned privacy policies and terms of use.

37. However, as described in Paragraphs 20-23, Respondent disclosed users' health information to numerous third parties authorized to use the data for advertising (among other uses). At no point did Respondent inform users that their health data could be used for these third parties' purposes.

Respondent's Failure to Provide Adequate Choice for Third-Party Use of Health Information for Advertising, Product Improvement, and Other Purposes

38. Privacy Shield Principle 2, "Choice," requires organizations to "offer individuals the opportunity to choose (opt out) whether their personal information is ... to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals." Principle 2(a).

39.

47. Respondent also violated Principle 3 because it did not take reasonable and appropriate steps to ensure processing of users' information consistent with the Principles. Specifically, as described in Paragraph 22, Respondent did not require third parties it considered agents, including Facebook, Google, Fabric, and AppsFlyer, to sign any contract acknowledging that they could or would receive Flo App users' health information or requiring processing consistent with the sensitivity of this information. To the contrary, as described in Paragraph 21, Respondent agreed to terms of service that specifically prohibited disclosures of health information to Facebook and AppsFlyer.

48. As a result, these third parties were not even aware that they had received Flo App users' health data and, therefore, could not process the data in a manner consistent with its sensitivity.

Respondent's Failure to Abide by the Principle of Purpose Limitation

49. Privacy Shield Principle 5, "Data Integrity and Purpose Limitation," provides, in part: "An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual." Principle 5(a).

50. Respondent collected health information from Flo App users for the purpose of providing the Flo App's functions. By disclosing Flo App users' health information to third parties under

Facebook, and Fabric. Therefore, the represent

62. In fact, as described in Paragraphs 45-48, Respondent did not adhere to the Privacy Shield Principle of Accountability for Onward Transfers. Therefore, the representation set forth in Paragraph 61 is false or misleading.

Count VII

Misrepresentation Reg