James M. Wagstaffe (95535)
Frank Busch (258288)
**WAGSTAFFE, VON LOEWENFELDT, BUSCH & RADWICK LLP**
100 Pine Street, Suite 725
San Francisco, CA 94111
Tel: (415) 357-8900
Fax: (415) 357-8910
wagstaffe@wvbrlaw.com
busch@wvbrlaw.com

*Counsel for Plaintiffs Erica Frasco and Sarah Wellman*

Christian Levis (*pro hac vice*)
Amanda Fiorilla (*pro hac vice*)
**LOWEY DANNENBERG, P.C.**
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

*Proposed Interim Co-Lead Counsel for Plaintiffs and the Proposed Class*

Carol C. Villegas (*pro hac vice*)
Michael Canty (*pro hac vice*)
**LABATON SUCHAROW LLP**
140 Broadway
New York, NY 10005
Tel: (212) 907-0700
Fax: (212) 818-0477
cvillegas@labaton.com
mcanty@labaton.com

*Proposed Interim Co-Lead Counsel for Plaintiffs and the Proposed Class*

Diana J. Zinser (*pro hac vice*)
**SPECTOR ROSEMAN & KODROFF, P.C.**
2001 Market Street, Suite 3420
Philadelphia, PA 19103
Tel: (215) 496-0300
Fax: (215) 496-6611
dzinser@srkattorneys.com

*Proposed Interim Co-Lead Counsel for Plaintiffs and the Proposed Class*

**UNITED STATES DISTRICT COURT**
**NORTHERN DISTRICT OF CALIFORNIA**

ERICA FRASCO, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FLO HEALTH, INC., GOOGLE, LLC, FACEBOOK, INC., APPSFLYER, INC., and FLURRY, INC.,

Defendants.

Case No.: 3:21-cv-00757-JD

**CONSOLIDATED CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

SARAH WELLMAN, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FLO HEALTH, INC., GOOGLE, LLC, FACEBOOK, INC., APPSFLYER, INC., and FLURRY, INC.,

Defendants.

JUSTINE PIETRZYK, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FLO HEALTH, INC., GOOGLE, LLC, FACEBOOK, INC., APPSFLYER, INC., and FLURRY, INC.,

Defendants.

JENNIFER CHEN, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FLO HEALTH, INC., GOOGLE, LLC, FACEBOOK, INC., APPSFLYER, INC., and FLURRY, INC.,

Defendants.

TESHA GAMINO, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FLO HEALTH, INC., GOOGLE, LLC, FACEBOOK, INC., APPSFLYER, INC., and FLURRY, INC.,

Defendants.

LEAH RIDGWAY and AUTUMN MEIGS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FLO HEALTH, INC., GOOGLE, LLC, FACEBOOK, INC., APPSFLYER, INC., and FLURRY, INC.,

Defendants.

MADELINE KISS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FLO HEALTH, INC., GOOGLE, LLC, FACEBOOK, INC., APPSFLYER, INC., and FLURRY, INC.,

Defendants.

Plaintiffs Erica Frasco, Sarah Wellman, Justine Pietrzyk, Jennifer Chen, Tesha Gamino, Leah Ridgway, Autumn Meigs, and Madeline Kiss ("Plaintiffs"), on behalf of themselves and all others similarly situated, assert the following against Defendants Flo Health, Inc. ("Flo Health"), Google, LLC ("Google"), Facebook, Inc. ("Facebook"), AppsFlyer, Inc. ("AppsFlyer"), and Flurry, Inc. ("Flurry")[1] based upon personal knowledge, where applicable, information and belief, and the investigation of counsel, which included, among other things, consultation with experts in the field of data privacy.

## SUMMARY OF ALLEGATIONS

1. Defendant Flo Health owns and developed the Flo Period & Ovulation Tracker ("Flo App" or "App"), one of the most popular health and fitness mobile applications.

2. The Flo App purports to use artificial intelligence to provide advice and assistance related to women's health, such as by serving as an ovulation calendar, period tracker, pregnancy guide, and wellness and lifestyle tracker.

3. Flo Health touts that its app is the "#1 mobile product for women's health." The Flo App has been installed more than 180 million times and has more than 38 million monthly active users. The App has also been rated the #1 period tracker in the United States based on active audience and as the #1 most downloaded health app in the Apple App Store.[2]

4. The Flo App presents itself as a leader in women's health care with at least "60 doctors and experts from Europe and North America" on its Medical Board.[3]

5. In order to use the Flo App, millions of users—including Plaintiffs—provide Flo Health with personally identifying information (e.g., their names, email addresses, dates of birth, and places of residence), along with intimate details about their sexual health, menstruation cycles,

---

[1] Defendants Flo Health, Google, Facebook, Appsflyer, and Flurry are hereafter referred to collectively, at times, as "Defendants." Defendants Google, Facebook, Appsflyer, and Flurry are hereafter referred to, collectively, at times, as the "Non-Flo Defendants."

[2] The Flo App was also featured as the "App of the Day" in the Apple App Store in over 30 countries.

[3] *Our Medical Expertise*, FLO HEALTH, INC., https://flo.health/medical-expertise.

gynecological health, and physical well-being through a series of "survey questions." These questions cover extremely personal topics and include, for example: (1) "do you experience any pain during sex?" (2) "how often do you have sex?" (3) "how often do you masturbate?" (4) "have you noticed a decrease in sexual desire?" (5) "are you sexually active during your period?" and (6) "what type of relationship do you have at present?"

6. Users also provided intimate, personal health details in response to probing survey questions about health and wellness, such as: (1) "do you smoke" (2) "how often do you experience stress?" (3) "do you want to change your weight?" (4) "do you follow a particular diet?" (5) "how often do you exercise?" (6) "do you get yeast infections?" (6) "do you have any chronic diseases?" and (7) "do you have any reproductive system diseases?"

7. Within the first few minutes of using the Flo App, users answer over thirty survey questions like these. As users continue to use the app, they are encouraged by Flo Health to provide more and more intimate health data, including daily information about whether they have their period, their weight, how long they slept, whether they had sex (as well as their sex drive, if sex was unprotected, or if they masturbated), their mood (ranging from "calm" to "very self-critical") and if they have any health symptoms (such as headaches, breast tenderness, acne, or fatigue).

8. With access to this highly sensitive information, Flo Health claims to predict ovulation, aid in pregnancy and childbirth, and provide lifestyle and wellness suggestions, allowing users to "take full control of [their] health."

9. Plaintiffs and Class members provided this information to Flo Health based on the company's repeated assurances that their intimate health data would remain protected and confidential and would not be disclosed to third parties.

10. This is because the improper collection and surreptitious sharing of this intimate data has significant real-world consequences. Indeed, in today's world, data is an extremely valuable commodity. The companies that deal in this data—such as Defendants Google and Facebook—are some of the largest and most valuable companies in the world. When these companies gain access to the intimate data users shared here, they are able to capitalize on an especially sensitive class of

information and use this information for their own benefit, including targeting women with ads in ways that are acutely invasive.

11. Flo Health's privacy policies and public assurances have claimed—time and time again—that Flo Health would not share users' intimate health data with ***anyone***. Flo Health's website touts that "[p]rivacy in the digital age is of utmost importance. Flo provides a secure platform for millions of women globally."[4]

12. Similarly, Flo Health's Privacy Policy stated, and has historically stated, in all capital letters, that it "WILL NOT TRANSMIT ANY OF YOUR PERSONAL DATA TO THIRD PARTIES, EXCEPT IF IT IS REQUIRED TO PROVIDE THE SERVICE TO YOU (E.G. TECHNICAL SERVICE PROVIDERS), UNLESS WE HAVE ASKED FOR YOUR EXPLICIT CONSENT." Flo Health assured users that these third parties, including the Non-Flo Defendants, would not receive "survey results," i.e., the answers to Flo Health's probing health questions, "information regarding your marked cycles, pregnancy, symptoms, notes," or information about "which articles [users] view," i.e., users' intimate health data. Flo Health further assured users that third parties, including the Non-Flo Defendants, with whom it shared data "w[ould] never use such information for any other purpose except to provide services in connection with the App."[5]

13. Contrary to these assurances, Flo Health knowingly collected, transmitted, and disclosed Plaintiffs' and Class members' intimate health data to third parties, including the Non-Flo Defendants.

14. Flo Health disclosed its users' highly sensitive health information to the Non-Flo Defendants and other third parties through "software development kits" ("SDKs") that it incorporated into the Flo App. SDKs are a collection of tools and programs that allow app developers, like Flo Health, to add functionality or features to their app that are developed by third parties.

---

[4] *About Us*, FLO HEALTH, INC., https://flo.health/our-mission (last visited Sept. 1, 2021).

[5] *Privacy Policy*, FLO HEALTH, INC. (effective May 25, 2018), https://flo.health/privacy-policy-archived/may-25-2018.

15. For instance, Facebook's SDK can be incorporated into an app to share user data between an app and Facebook. By using the Facebook SDK, developers can gain access to Facebook's data analytics and use Facebook tools to assist with mobile ads, among other things.

16. Flo Health incorporated Facebook's SDK so that it could use Facebook's analytics tools to identify which of its users would be prime targets for advertisements keyed off the data they entered into the App. Flo Health incorporated similar SDKs from all the Non-Flo Defendants, who are all marketing and analytics firms or advertisers.

17. In exchange for using the Non-Flo Defendants' SDKs, Flo Health transmitted intimate health data entered into the Flo App to the Non-Flo Defendants—in direct contravention of Flo Health's assurances to users that this information would not be disclosed—including when a user indicated that they were on their period or intended to get pregnant.

18. The Non-Flo Defendants, including two of the largest digital advertisers in the world, incorporated this information into their existing data analytics and research segments to compile profiles and target users for advertisements.

19. The Non-Flo Defendants' access and use of this information can and do have profound consequences that users of the Flo App would never anticipate. For instance, armed with knowledge that a Flo App user is pregnant or attempting to get pregnant, the Non-Flo Defendant can specifically target that user with ads for prenatal vitamins, breast pumps, or fertility treatments, among other things. In some instances, Flo Health may know a user is pregnant—based on the user's data—before the user herself. Because this information was shared with the Non-Flo Defendants, users could be targeted for ads that the users may find overwhelming or disturbing, depending on whether they did or did not intend to get pregnant. As another example, if a user indicated that she experienced oily skin during her menstruation cycle, the Non-Flo Defendants could use this information to target that user (i.e., Plaintiffs and Class members) with advertisements for certain skin care products around this time period. The intimate health data entered into the Flo Health App is some of the most private information about a user and was provided under the guise that this

information would stay private—not to develop profiles about users or target them for advertisements.

20. The Non-Flo Defendants knew that the data collected and received from Flo Health included intimate health data—but they did nothing to stop Flo Health from sharing this information because it is vital to their business. By continuing to contract with Flo Health to receive this data—and using this data for their own purposes—the Non-Flo Defendants (as well as Flo Health) intentionally intruded upon Plaintiffs' and Class members' privacy.

21. The truth about Flo Health's and the Non-Flo Defendants' conduct was discussed in a report published by the *Wall Street Journal* in February 2019, revealing that despite Flo Health's promises that it would not share intimate health data, Flo Health had spent years disclosing the intimate health data that users entered into the Flo App to dozens of third parties, including the Non-Flo Defendants who were free to use this data for their own purposes, without limitation.

22. In response to the revelation that Flo Health was sharing users' intimate health data with the Non-Flo Defendants, the Federal Trade Commission ("FTC") launched its own investigation into Flo Health's data privacy and disclosure practices and ultimately filed a complaint, charging Flo Health with making a variety of fraudulent misrepresentations to Flo App users in violation of their privacy rights.

23. Likewise, the New York State Department of Financial Services ("NYSDFS"), at the direction of New York Governor Andrew M. Cuomo, opened an investigation into Facebook concerning its collection of sensitive data for its own advertising and marketing purposes—including intimate health data from Flo Health users. Governor Cuomo characterized the practice as an "outrageous abuse of privacy."[6]

[6] *Report on Investigation of Facebook Inc. Data Privacy Concerns*, N.Y. STATE DEP'T OF FIN. SERVS. (Feb. 18, 2021), https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf.

24. Members of Congress expressed outrage as well, with Senator Ed Markey of Massachusetts calling the behavior a "new low in privacy malpractice."[7]

25. On January 13, 2021, Flo Health entered into a settlement with the FTC that prohibited Flo Health from further misrepresenting the purposes for which or entities to whom it discloses users' intimate health data, as well as obtain an independent review of its Privacy Policy, obtain user consent before sharing their data, and notify third parties that previously received users' intimate health data to destroy that information.[8]

26. NYSDFS released a report on February 18, 2021, detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of intimate health data from Flo Health users. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive health data, Facebook received, stored, and analyzed this data anyway, including intimate health data from Flo App users. Facebook was unwilling to review the data it previously collected and analyzed and so the NYSDFS called on federal regulators to compel Facebook to undergo such a process.

27. If Plaintiffs and Class members had known that Flo Health would share their intimate health data with Non-Flo Defendants, they would not have used the Flo App.

28. Defendants' actions constitute an extreme invasion of Plaintiffs' and Class members' right to privacy and violate federal and state statutory and common law.

## JURISDICTION AND VENUE

29. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than 100 putative class members defined below, and minimal diversity

---

[7] Sam Schechner, *Popular Apps Cease Sharing Data With Facebook*, WALL ST. J. (Feb. 24, 2019).

[8] *Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Mislead Consumers About the Disclosure of their Health Data*, FTC (Jan. 13, 2021), https://www.ftc.gov/news-events/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc.

exists because a significant portion of putative class members are citizens of a state different from the citizenship of at least one Defendant.

30. This Court also has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 since this suit is brought under the laws of the United States, i.e., the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.* and the Federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq.*, and supplemental jurisdiction pursuant to 28 U.S.C. § 1367 over the remaining state common law and statutory claims as these state law claims are part of the same case or controversy as the federal statutory claim over which the Court has original jurisdiction.

31. This Court has specific personal jurisdiction over Flo Health because it consented to jurisdiction in this District in its Terms of Use, which states:

> Any dispute arising from this Agreement shall be governed by the laws of the State of California without regard to its conflict of law provisions. **SOLE AND EXCLUSIVE JURISDICTION FOR ANY ACTION OR PROCEEDING ARISING OUT OF OR RELATED TO THIS AGREEMENT SHALL BE IN AN APPROPRIATE STATE OR FEDERAL COURT LOCATED IN SAN FRANCISCO COUNTY, STATE OF CALIFORNIA** . . . .[9]

32. This Court has general personal jurisdiction over the Non-Flo Defendants because they each maintain their principal place of business in California. Additionally, the Non-Flo Defendants are subject to specific personal jurisdiction in this State because a substantial part of the events and conduct giving rise to Plaintiffs' claims occurred in this State.

33. Venue is proper in this District pursuant to 28 U.S.C. §1391(b), (c), and (d) because Flo Health transacts business in this District and a substantial portion of the events giving rise to the claims occurred in this District.

34. Intra-district Assignment: A substantial part of the events and omissions giving rise to the violations of law alleged herein occurred in the County of San Francisco, and as such, this action may properly be assigned to the San Francisco or Oakland divisions of this Court pursuant to Civil Local Rule 3-2(c).

---

[9] *Terms of Use*, FLO HEALTH, INC. (effective Feb. 5, 2020) (emphasis in original), https://flo.health/terms-of-service.

## PARTIES

### A. Plaintiffs

#### a. Erica Frasco

35. Plaintiff **Erica Frasco** is a natural person and citizen of New Jersey and a resident of Passaic County.

36. Plaintiff Frasco downloaded the Flo App from the Apple app store in or around 2017 and has been an active user ever since.

37. Plaintiff Frasco provided Flo Health with her intimate health data, including information and/or symptoms about her health and wellness, menstruation cycle, and sexual activity.

38. Plaintiff Frasco believed that her intimate health data would stay private and that Flo Health would not disclose this information to third parties, including the Non-Flo Defendants. Plaintiff Frasco did not consent or provide permission for Flo Health to share or disclose this information.

39. In direct contravention to its Privacy Policy and public assurances, Flo Health disclosed Plaintiff Frasco's intimate health data without her knowledge or consent to third parties, including the Non-Flo Defendants.

40. By the nature of Flo Health's concealment, Plaintiff Frasco was not provided notice and did not have the opportunity to provide consent to Flo Health's disclosure of her data to the Non-Flo Defendants and the use of her intimate health data by Flo Health and the Non-Flo Defendants for their own benefit. Namely, the Non-Flo Defendants used users' intimate health data, including Plaintiff Frasco's, for their own purposes and in some cases to generate revenue by selling targeted advertising to customers based on profiles on Flo Health users that were developed based on their sensitive health data.

41. Plaintiff Frasco would not have used the Flo App if she had known that Flo Health would share her intimate health data with third parties, including the Non-Flo Defendants.

b. **Sarah Wellman**

42. Plaintiff **Sarah Wellman** is a natural person and citizen of California and a resident of Sonoma County.

43. Plaintiff Wellman downloaded the Flo App from the Apple app store in or around 2018 and was an active user until March 2020.

44. Plaintiff Wellman provided Flo Health with her intimate health data, including information and/or symptoms about her health and wellness, menstruation cycle, and sexual activity.

45. Plaintiff Wellman believed that her intimate health data would stay private and that Flo Health would not disclose this information to third parties, including the Non-Flo Defendants. Plaintiff Wellman did not consent or provide permission for Flo Health to share or disclose this information.

46. In direct contravention to its Privacy Policy and public assurances, Flo Health disclosed Plaintiff Wellman's intimate health data without her knowledge or consent to third parties, including the Non-Flo Defendants.

47. By the nature of Flo Health's concealment, Plaintiff Wellman was not provided notice and did not have the opportunity to provide consent to Flo Health's disclosure of her data to the Non-Flo Defendants and the use of her intimate health data by Flo Health and the Non-Flo Defendants for their own benefit. Namely, the Non-Flo Defendants used users' intimate health data, including Plaintiff Wellman's, for their own purposes and in some cases to generate revenue by selling targeted advertising to customers based on profiles on Flo Health users that were developed based on their sensitive health data.

48. Plaintiff Wellman would not have used the Flo App if she had known that Flo Health would share her intimate health data with third parties, including the Non-Flo Defendants.

c. **Justine Pietrzyk**

49. Plaintiff Justine Pietrzyk ("Plaintiff Pietrzyk") is a natural person and citizen of Pennsylvania and resident of Philadelphia County.

50. Plaintiff Pietrzyk downloaded the Flo App from the Apple app store in or around January 2020 and was an active user until about February 2021.

51. Plaintiff Pietrzyk provided Flo Health with her intimate health data, including information and/or symptoms about her health and wellness, menstruation cycle, and sexual activity.

52. Plaintiff Pietrzyk believed that her intimate health data would stay private and that Flo Health would not disclose this information to third parties, including the Non-Flo Defendants. Plaintiff Pietrzyk did not consent or provide permission for Flo Health to share or disclose this information.

53. In direct contravention to its privacy policy and public assurances, Flo Health disclosed Plaintiff Pietrzyk's intimate health data without her knowledge or consent to third parties, including the Non-Flo Defendants.

54. By the nature of Flo Health's concealment, Plaintiff Pietrzyk was not provided notice and did not have the opportunity to provide consent to Flo Health's disclosure of her data to the Non-Flo Defendants and the use of her intimate health data by Flo Health and the Non-Flo Defendants for their own benefit. Namely, the Non-Flo Defendants used users' intimate health data, including Plaintiff Pietrzyk's, for their own purposes and in some cases to generate revenue by selling targeted advertising to customers based on profiles on Flo Health users that were developed based on their sensitive health data.

55. Plaintiff Pietrzyk would not have used the Flo App if she had known that Flo Health would share her intimate health data with third parties, including the Non-Flo Defendants.

d. **Jennifer Chen**

56. Plaintiff **Jennifer Chen** is a natural person and citizen of California and a resident of Placer County.

57. Plaintiff Chen downloaded the Flo App from the Apple app store in or around 2017 and has been an active user ever since.

58. Plaintiff Chen provided Flo Health with her intimate health data, including information and/or symptoms about her health and wellness, menstruation cycle, and ovulation for natural family planning.

59. Plaintiff Chen believed that her intimate health data would stay private and that Flo Health would not disclose this information to third parties, including the Non-Flo Defendants. Plaintiff Chen did not consent or provide permission for Flo Health to share or disclose this information.

60. In direct contravention to its Privacy Policy and public assurances, Flo Health disclosed Plaintiff Chen's intimate health data without her knowledge or consent to third parties, including the Non-Flo Defendants.

61. By the nature of Flo Health's concealment, Plaintiff Chen was not provided notice and did not have the opportunity to provide consent to Flo Health's disclosure of her data to the Non-Flo Defendants and the use of her intimate health data by Flo Health and the Non-Flo Defendants for their own benefit. Namely, the Non-Flo Defendants used users' intimate health data, including Plaintiff Chen's, for their own purposes and in some cases to generate revenue by selling targeted advertising to customers based on profiles on Flo Health users that were developed based on their sensitive health data.

62. Plaintiff Chen would not have used the Flo App if she had known that Flo Health would share her intimate health data with third parties, including the Non-Flo Defendants.

e. **Tesha Gamino**

63. Plaintiff **Tesha Gamino** is a natural person and citizen of California and a resident of Riverside County.

64. Plaintiff Gamino downloaded the Flo App from the Apple app store in or around 2016 and has been an active user ever since.

65. Plaintiff Gamino provided Flo Health with her intimate health data, including information and/or symptoms about her health and wellness, menstruation cycle, and sexual activity.

66. Plaintiff Gamino believed that her intimate health data would stay private and that Flo Health would not disclose this information to third parties, including the Non-Flo Defendants. Plaintiff Gamino did not consent or provide permission for Flo Health to share or disclose this information.

67. In direct contravention to its Privacy Policy and public assurances, Flo Health disclosed Plaintiff Gamino's intimate health data without her knowledge or consent to third parties, including the Non-Flo Defendants.

68. By the nature of Flo Health's concealment, Plaintiff Gamino was not provided notice and did not have the opportunity to provide consent to Flo Health's disclosure of her data to the Non-Flo Defendants and the use of her intimate health data by Flo Health and the Non-Flo Defendants for their own benefit. Namely, the Non-Flo Defendants used users' intimate health data, including Plaintiff Gamino's, for their own purposes and in some cases to generate revenue by selling targeted advertising to customers based on profiles on Flo Health users that were developed based on their sensitive health data.

69. Plaintiff Gamino would not have used the Flo App if she had known that Flo Health would share her intimate health data with third parties, including the Non-Flo Defendants.

f. **Leah C. Ridgway**

70. Plaintiff **Leah C. Ridgway** is a natural person and citizen of Ohio and a resident of Franklin County.

71. Plaintiff Ridgway downloaded the Flo App from the Apple app store in or around March 2018 and has been an active user ever since.

72. Plaintiff Ridgway provided Flo Health with her intimate health data, including information and/or symptoms about her health and wellness, menstruation cycle, sexual activity, and pregnancy.

73. Plaintiff Ridgway believed that her intimate health data would stay private and that Flo Health would not disclose this information to third parties, including the Non-Flo Defendants.

Plaintiff Ridgway did not consent or provide permission for Flo Health to share or disclose this information.

74. In direct contravention to its Privacy Policy and public assurances, Flo Health disclosed Plaintiff Ridgway's intimate health data without her knowledge or consent to third parties, including the Non-Flo Defendants.

75. By the nature of Flo Health's concealment, Plaintiff Ridgway was not provided notice and did not have the opportunity to provide consent to Flo Health's disclosure of her data to the Non-Flo Defendants and the use of her intimate health data by Flo Health and the Non-Flo Defendants for their own benefit. Namely, the Non-Flo Defendants used users' intimate health data, including Plaintiff Ridgway's, for their own purposes and in some cases to generate revenue by selling targeted advertising to customers based on profiles on Flo Health users that were developed based on their sensitive health data.

76. Plaintiff Ridgway would not have used the Flo App if she had known that Flo Health would share her intimate health data with third parties, including the Non-Flo Defendants.

g. **Autumn N. Meigs**

77. Plaintiff **Autumn N. Meigs** is a natural person and citizen of Ohio and a resident of Stark County.

78. Plaintiff Meigs downloaded the Flo App from the Apple app store in or around April 2018 and has been an active user ever since. At the time Plaintiff Meigs began using the Flo App, Plaintiff Meigs was a minor.

79. Plaintiff Meigs provided Flo Health with her intimate health data, including information and/or symptoms about her health and wellness and menstruation cycle.

80. Plaintiff Meigs believed that her intimate health data would stay private and that Flo Health would not disclose this information to third parties, including the Non-Flo Defendants. Plaintiff Meigs did not consent or provide permission for Flo Health to share or disclose this information.

81. In direct contravention to its Privacy Policy and public assurances, Flo Health disclosed Plaintiff Meigs' intimate health data without her knowledge or consent to third parties, including the Non-Flo Defendants.

82. By the nature of Flo Health's concealment, Plaintiff Meigs was not provided notice and did not have the opportunity to provide consent to Flo Health's disclosure of her data to the Non-Flo Defendants and the use of her intimate health data by Flo Health and the Non-Flo Defendants for their own benefit. Namely, the Non-Flo Defendants used users' intimate health data, including Plaintiff Meigs's, for their own purposes and in some cases to generate revenue by selling targeted advertising to customers based on profiles on Flo Health users that were developed based on their sensitive health data.

83. Plaintiff Meigs would not have used the Flo App if she had known that Flo Health would share her intimate health data with third parties, including the Non-Flo Defendants.

h. **Madeline Kiss**

84. Plaintiff Madeline Kiss is a natural person and citizen of New York and a resident of Kings County. From approximately February 2017 until June 2018, Plaintiff Kiss was a citizen of California and a resident of Orange County.

85. Plaintiff Kiss downloaded the Flo App from the Apple app store in or around spring of 2017 and was an active user until January 2021. Plaintiff Kiss used the app while residing in California and also while residing in New York.

86. Plaintiff Kiss provided Flo Health with her intimate health data, including information and/or symptoms about her health and wellness, menstruation cycle, and sexual activity.

87. Plaintiff Kiss believed that her intimate health data would stay private and that Flo Health would not disclose this information to third parties, including the Non-Flo Defendants. Plaintiff Kiss did not consent or provide permission for Flo Health to share or disclose this information.

88. In direct contravention to its Privacy Policy and public assurances, Flo Health disclosed Plaintiff Kiss' intimate health data without her knowledge or consent to third parties, including the Non-Flo Defendants.

89. By the nature of Flo Health's concealment, Plaintiff Kiss was not provided notice and did not have the opportunity to provide consent to Flo Health's disclosure of her data to the Non-Flo Defendants and the use of her intimate health data by Flo Health and the Non-Flo Defendants for their own benefit. Namely, the Non-Flo Defendants used users' intimate health data, including Plaintiff's, for their own purposes and in some cases to generate revenue by selling targeted advertising to customers based on profiles on Flo Health users that were developed based on their sensitive health data.

90. Plaintiff Kiss would not have used the Flo App if she had known that Flo Health would share her intimate health data with third parties, including the Non-Flo Defendants.

**B. Defendants**

91. Defendant **Flo Health, Inc.** is a Delaware corporation with principal executive offices located at 1013 Centre Road, Suite 403-B, Wilmington, Delaware 19805.

92. In direct contravention of Flo Health's assurances, Flo Health knowingly collected and shared Plaintiffs' and Class members' intimate health data with the Non-Flo Defendants.

93. Defendant **Google, LLC** is a Delaware limited liability company with principal executive offices located at 1600 Amphitheatre Parkway Mountain View, California 94043. Google is an advertising company that "make[s] money" from "advertising products [that] deliver relevant ads at just the right time," generating "revenues primarily by delivering both performance advertising and brand advertising."[10] Indeed in 2020, Google generated $146.9 billion in advertising revenue, which amounted to more than 80 percent of Google's total revenues for the year. Google generated an even higher percentage of its total revenues from advertising in prior years:

[10] Alphabet Inc. SEC Form 10-K for fiscal year ended December 31, 2020, https://www.sec.gov/Archives/edgar/data/1652044/000165204421000010/goog-20201231.htm.

| Year | Total Revenue | Ad Revenue | % Ad Revenue |
|---|---|---|---|
| 2020 | $182.5 billion | $146.9 billion | 80.49% |
| 2019 | $161.9 billion | $134.8 billion | 83.29% |
| 2018 | $136.8 billion | $116.5 billion | 85.12% |
| 2017 | $110.9 billion | $95.6 billion | 86.21% |

94. In 2017, Google acquired Fabric, a company that provides SDKs to developers that they can incorporate into their apps. [11] Flo Health incorporated the Fabric SDK into the Flo App.

95. Flo Health knew that the data it provided to Google through the Fabric SDK would be used for Google's own purposes. The Fabric Software and Services Agreement, which Flo Health agreed to, stated: "[Flo Health] acknowledges and agrees that Google [Fabric] may use Usage Data for its own business purposes," where "Usage Data" was defined to mean "all information, data and other content, not including any [identifying data], received by Google related to [Flo Health]'s use of the Fabric Technology."

96. Google offers a separate SDK through Google Analytics. Flo Health incorporated Google's SDK into the Flo App.

97. Flo Health knew that the data it provided to Google through the Google Analytics SDK would be used for Google's own purposes. The Terms of Service of Google Analytics, which Flo Health agreed to, stated: "Google and its wholly owned subsidiaries may retain and use ... information collected in [Flo Health's] use of the Service."

98. Google Analytics' Terms of Services prohibited companies like Flo Health from "pass[ing] information to Google that Google could use or recognize as personally identifiable information." Google's Privacy Policy also informs users that it does not use the information it collects to "show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health."[12]

---

[11] Fabric's operations and employees merged with Firebase after being acquired by Google. *See* Josh Costine, *Google acquires Fabric developer platform and team from Google*, TECH CRUNCH (Jan. 18, 2017), https://techcrunch.com/2017/01/18/google-twitter-fabric/.

[12] *Privacy Policy*, GOOGLE, LLC, https://policies.google.com/privacy#footnote-sensitive-categories (last visited Sept. 1, 2021).

99. As one of the largest advertisers and data analytics companies in the country, Google knew that the data it received from Flo Health through Fabric and Google Analytics contained intimate health data. Despite knowing this, Google continued to receive, analyze, and use this information for its own purposes, including marketing and data analytics.

100. Defendant **Facebook, Inc**. is a Delaware corporation with principal executive offices located at 1601 Willow Road, Menlo Park, California 94025. Facebook is a social media platform that—as the chart below illustrates—"generate[s] substantially all of [its] revenue from selling advertising placements to marketers."[13]

| Year | Total Revenue | Ad Revenue | % Ad Revenue |
|---|---|---|---|
| 2020 | $85.97 billion | $84.17 billion | 97.90% |
| 2019 | $70.70 billion | $69.66 billion | 98.52% |
| 2018 | $55.84 billion | $55.01 billion | 98.51% |
| 2017 | $40.65 billion | $39.94 billion | 98.25% |

101. Facebook offers an SDK to developers, like Flo Health, that allows developers to see certain statistics about a users' activity in the app and target users for ads on Facebook. Flo Health incorporated the Facebook SDK into the Flo App.

102. Facebook has described how its SDKs work as follows: "Developers can receive analytics that allow them to understand what the audience of their app enjoys and improve their apps over time. Developers may also use Facebook services to monetise their apps through Facebook Audience Network. Subject to that Facebook user's prior consent, Facebook may also use this data to provide that user with more personalised ads."[14]

103. Flo Health knew that the data it provided to Facebook through the Facebook SDK would be used for Facebook's own purposes. Facebook's Business Tools Terms, which Flo Health

---

[13] Facebook, Inc. SEC Form 10-K for fiscal year ended December 31, 2020, https://www.sec.gov/Archives/edgar/data/1326801/000132680120000013/fb-12312019x10k.htm.

[14] *No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data*, PRIVACY INTERNATIONAL (Sept. 9, 2019), https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data.

agreed to, stated: "We use [aggregated data] to personalize the features and content (including ads and recommendations) we show people on and off our Facebook Company Products . . . We may also use [data] . . . for research and development purposes, and to . . . improve the Facebook Company Products." Even though Facebook claims to use the data in aggregated form, according to the *Wall Street Journal*, Facebook can match that data with actual Facebook users.

104. While Facebook had a policy requesting that developers not share health-related info with the company, Facebook received, stored, and analyzed Flo Health users' intimate health data anyway.

105. As one of the largest advertisers in the nation, Facebook knew that the data it received from Flo Health through the Facebook SDK contained intimate health data. Despite knowing this, Facebook continued to receive, analyze, and use this information for its own purposes, including marketing and data analytics.

106. Defendant **AppsFlyer, Inc.** is a Delaware corporation with principal executive offices located at 100 First Plaza, 100 1st Street, San Francisco, California 94105. AppsFlyer's core services include attribution, marketing analytics, and cost aggregation. According to the company's website, AppsFlyer has over 1,000 employees, 89,000 active mobile apps, and more than 9,000 tech partner integrations, with customers including Facebook and Google.[15]

107. AppsFlyer offers an SDK to developers, which Flo Health incorporated into the Flo App.

108. Flo Health knew that the data it provided to AppsFlyer through the AppsFlyer SDK would be used for AppsFlyer's own purposes. AppsFlyer's Terms of Use, which Flo Health agreed to, stated: "You hereby allow AppsFlyer to collect, store, use and process Customer Data," where "Customer Data" was defined to include "data concerning the characteristics and activities" of app users.

---

[15] *This is AppsFlyer*, APPSFLYER, INC., https://www.appsflyer.com/we-are-appsflyer/ (last visited Sept. 1, 2021).

109. While AppsFlyer had a policy requesting that developers not share sensitive information, like health information, AppsFlyer continued to receive Flo Health users' intimate health data anyway.

110. AppsFlyer, as one of the most prominent data attribution and marketing companies, knew that the data it received from Flo Health through the AppsFlyer SDK contained intimate health data. Despite knowing this, AppsFlyer continued to receive, analyze, and use this information for its own purposes, including marketing and data analytics.

111. Defendant **Flurry, Inc**. is a Delaware corporation with principal executive offices located at 110 5th Street, Suite 200, San Francisco, California 94103. Flurry helps app developers acquire, retain, and monetize audiences. Flurry touts that since 2008, "mobile app developers worldwide have relied on Flurry Analytics to unlock audience data, usage behavior, and monetization opportunities," reaching over 2 billion devices every month.[16]

112. Flurry offers an SDK to developers, which Flo Health incorporated into the Flo App.

113. Flo Health knew that the data it provided to Flurry through the Flurry SDK would be used for Flurry's own purposes. Flurry's Terms of Service, which Flo Health agreed to, states that: "As a condition of your access to the Services, you agree that Flurry has the right, for any purpose, to collect, retain, use, and publish in an aggregate manner . . . information collected in Your use of the Services, including without limitation . . . characteristics and activities of end users of your applications."

114. As one of the most prominent mobile app data analytics firms, Flurry knew that the data it received from Flo Health through Flurry contained intimate health data. Despite knowing this, Flurry continued to receive, analyze, and use this information for its own purposes, including marketing and analytics.

[16] *About Flurry*, FLURRY, INC., https://www.flurry.com/about/ (last visited Sept. 1, 2021).

## FACTUAL BACKGROUND

### A. Founding of Flo Health, Inc.

115. Flo Health began as a startup in 2015 owned by a group of mobile app developers based in Minsk, Belarus. That same year, the company released the Flo App, the first mobile application to make use of artificial intelligence to accurately predict reproductive cycles.

116. When first launched, the Flo App operated essentially as a calendar that allowed users to track their period and ovulation. Over time, the App's developers expanded the Flo App's functionality to assist with all phases of the reproductive cycle, including the start of menstruation, cycle tracking, preparation for conception, pregnancy, early motherhood, and menopause. The Flo App also expanded to provide users with overall health and wellness suggestions.

117. As the Flo App's features expanded, the App requested a wider and wider range of personal information from its users, including intimate personal details like a user's history of contraceptive methods, vaginal discharge, diseases, water intake, weight, pains and other physical or mental symptoms, mood swings, and sexual activity (including the users' sexual desire levels, whether they experience pain during sex, or did not use protection). Users can also write "personal notes" to log additional information in the App. As is often the case with apps that monetize user data, the Flo App was designed in such a way that encouraged users to share more and more intimate personal details about themselves. Flo Health also relied on push notifications to further encourage users to engage with the Flo App and turn over their information.

118. In 2017, Flo Health further expanded Flo App's functionality to include social media features alongside its services as a health product. The App's developers included a new community section on the App, allowing users to anonymously ask and answer questions related to women's health.

119. That same year, Flo Health gained international attention by working with the United Nations Population Fund as part of its "Let's Talk About it. Period." campaign, which aimed to increase public awareness of social and health issues related to menstruation.

120. Finally, by at least 2018, the Flo App purported to have a "Medical Board"—a team of health experts that assists in delivering accurate health information to Flo App users:

> With our team of scientists, doctors and health experts, we deliver content designed to empower women and help them make more informed decisions about their health and wellbeing.
>
> * * *
>
> Our medical board includes over 60 doctors and experts from Europe and North America, who are passionate about making accurate women's health information accessible to everyone. Our in-house medical team works closely with them to ensure that we deliver the most relevant and high-quality content to our users. Their areas of expertise include Obstetrics and Gynecology, Reproductive Endocrinology, Pediatrics, Nutrition, Neurology, Dermatology and more.[17]

121. Throughout this period, Flo App steadily grew more popular. By December 2020, 150 million users had downloaded the App. The App has been rated the #1 period tracker in the United States based on active audience and as the #1 most downloaded health app in the Apple App Store.

122. Through its success, Flo Health has gathered and collected intimate health data from more than 100 million users, including Plaintiffs. Users provided this information based on Flo Health's repeated assurances that users' intimate health data would remain private and that it would not be shared with third parties.

123. In fact, Flo Health affirmatively represented that it would, under no circumstances, share users' intimate health data without user consent. While Flo Health disclosed that it might share "certain" information with third parties who it uses to "supply software applications, web hosting and other technologies for the App," Flo Health promised this would not include "information regarding your marked cycles, pregnancy, symptoms, notes and other information entered by [users]" or "survey results" and "articles [users] view."

[17] *See supra*, note 3.

124. However, in February 2019, the *Wall Street Journal* released a bombshell report revealing for the first time that Flo Health shares its users' intimate health data with third parties, such as Defendant Facebook, including when a user was on her period or intended to get pregnant.[18]

125. Further investigations have revealed that Defendant Facebook was not the only third party with whom Flo Health disclosed consumers' intimate health data. Between at least 2016 and 2019, Flo Health contracted with numerous advertising and data analytics firms to provide, among other things, various marketing and analytics services in connection with the Flo App. These firms included the Non-Flo Defendants.

126. Despite Flo Health's representations that third parties would not receive users' survey results and "information regarding your marked cycles, pregnancy, symptoms, notes and other information entered by [users]," Flo Health disclosed users' intimate health data to the Non-Flo Defendants, including two of the largest advertising companies in the country.

127. Further, despite Flo Health's promise that third parties would only receive data "as necessary to perform their work" and "will never use such information for any other purpose except to provide services in connection with the App," Flo Health did not contractually limit how the Non-Flo Defendants could use this data.

128. In fact, the terms of service governing Flo Health's agreement with these third parties allowed the Non-Flo Defendants to receive, collect, and use the data for their own purposes, completely unrelated to services provided in connection with the Flo App. Indeed, when Flo Health disclosed Plaintiffs' and Class members' intimate health data with the Non-Flo Defendants, the Non-Flo Defendants utilized Plaintiffs and Class members' intimate health data for their own

[18] Sam Schechner and Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL ST. J. (Feb. 22, 2019 11:07 AM ET), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

purposes, including research and development—and in some cases, for marketing and advertising purposes. [19]

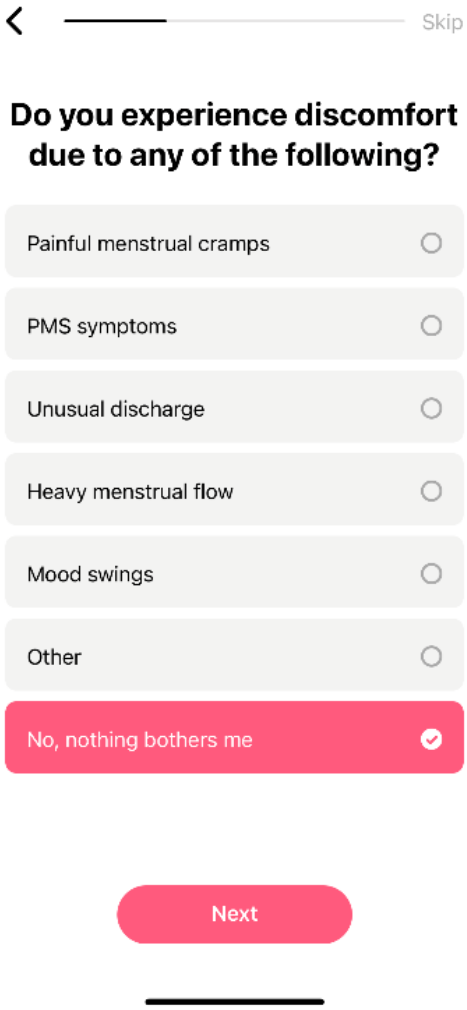
129. Flo Health entered into these contracts to disclose users' sensitive health data and did disclose this data without Plaintiffs' and Class members' knowledge or consent, in violation of their privacy rights and federal law.

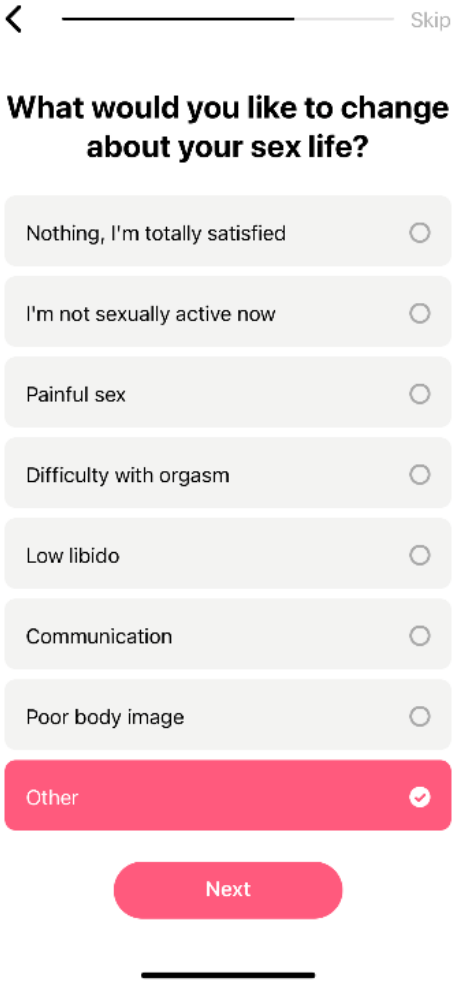
130. Likewise, through this deceit, Plaintiffs and Class members had no opportunity to provide consent to the Non-Flo Defendants' collection, analysis, and use of their intimate health data—for the Non-Flo Defendants' own benefit.

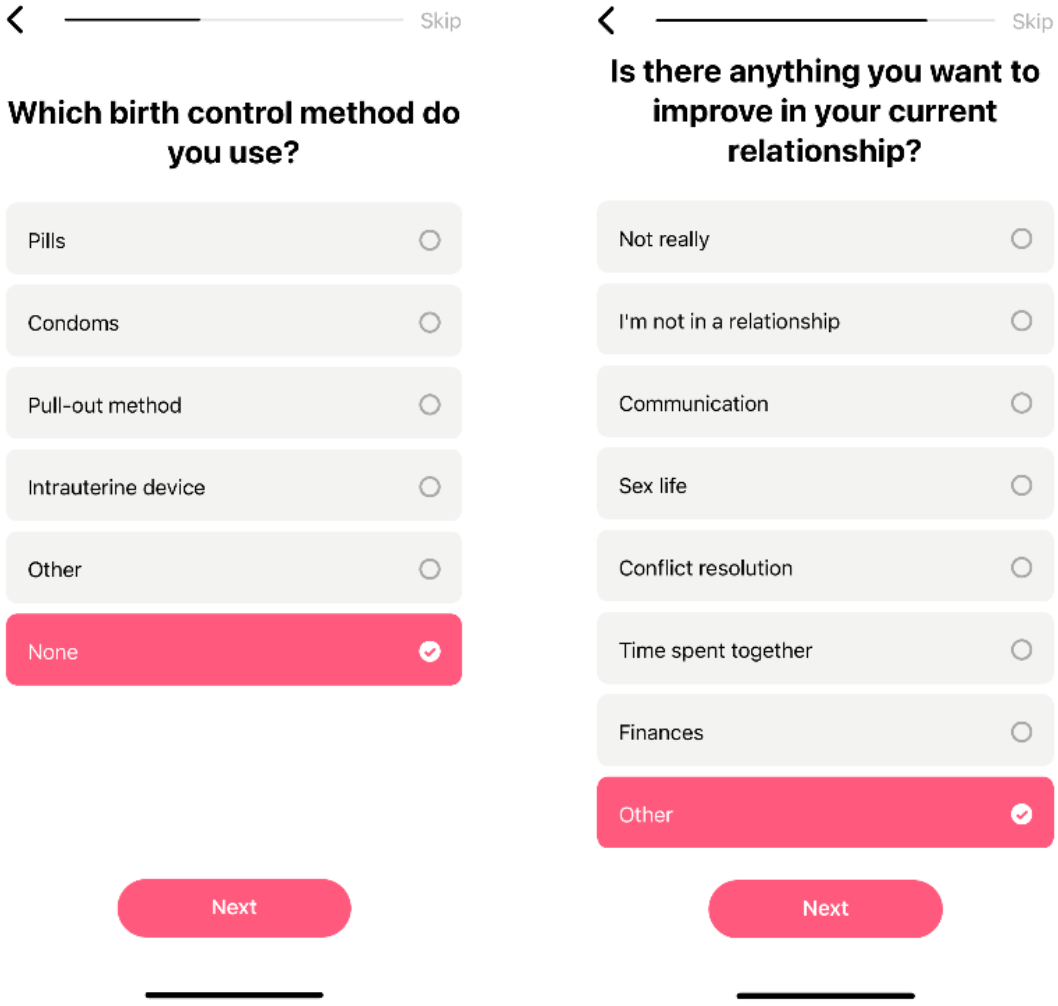
**B. Flo Health Designed Its App to Facilitate the Collection of Users' Private Data**

131. Flo Health designed the Flo App to request users to input intimate health and lifestyle-related information under the guise that they would receive better services. When a user creates a new account on the Flo App, the App will ask several questions related to the timing of the user's menstrual cycle, the discomfort of their menstrual cycle, mood swings, preferred birth control methods, reproductive health disorders, and their level of satisfaction with their sex life and romantic relationships. Some of these questions are reflected in the example screenshots below:

[19] Plaintiffs base the allegation that Facebook, Google, Flurry, and AppsFlyer specifically utilized personal health data for their own marketing and advertising purposes based upon reasonable inference due to: (1) the mechanics of how the SDKs and persistent identifiers work, and their intended purpose to transmit and receive information from third parties, as described herein; (2) the 2019 *Wall Street Journal* report which found that the Journal's testing revealed that "sensitive information was sent with a unique ***advertising*** identifier that can be matched to a device or profile"; (3) the fact that Facebook and Google's business model is predicated—and ***depends***—on advertising revenue as described in ¶¶ 93-105; (4) the FTC documents which detail how the SDKs described herein gather the unique "advertising" identifiers of the millions of Flo App users; (5) the fact that the FTC found that Flo Health entered into agreements with the Non-Flo Defendants which allowed them to "use any information obtained from Flo App users for the third party's own purposes, including, in certain cases, for advertising and product improvement"; and (6) the NYSDFS documents which specifically detailed how Facebook used SDKs , App Events, and Custom App Events—including the "sensitive user data being shared with Facebook, as reported in the WSJ Article"—to build a "marketing profile for each user" in order to advertise and generate revenue. The above list is non-exhaustive.


Skip
Do you experience discomfort due to any of the following?
Painful menstrual cramps
PMS symptoms
Unusual discharge
Heavy menstrual flow
Mood swings
Other
No, nothing bothers me
Next


Skip
What would you like to change about your sex life?
Nothing, I'm totally satisfied
I'm not sexually active now
Painful sex
Difficulty with orgasm
Low libido
Communication
Poor body image
Other
Next




132. The Flo App asks users to input more than 30 responses to intimate, personal questions like these all while setting up the App for the first time, including, but not limited to, the following:

a. How long have you been trying to conceive?

b. Do you have any reproductive diseases?

c. What medication are you currently taking? How often?

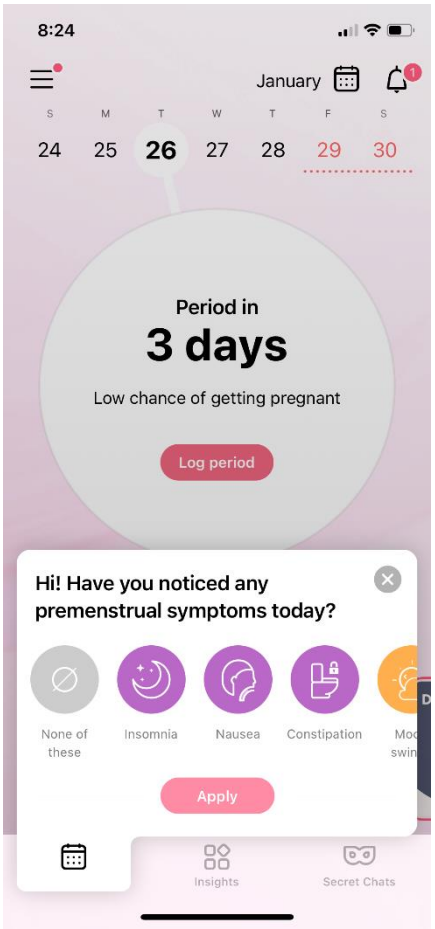
d. How often do you have sex?

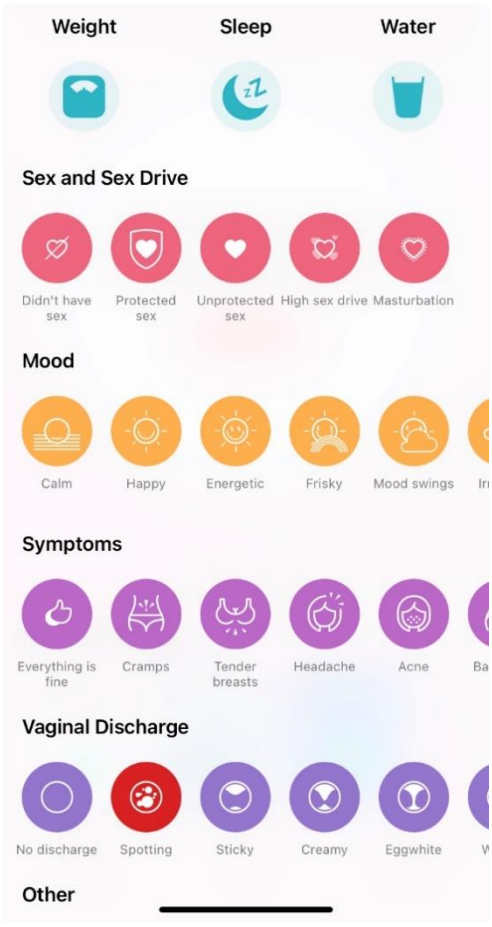
e. Do you experience any pain during sex?

f. How often do you masturbate?

g. Is it easy for you to orgasm?

133. The Flo App also regularly encourages users to update the App with vast quantities of additional intimate health-related information as they continue to use the App. For example, the interface of the Flo App suggests that users "[l]og 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 . . . ." As the screenshots below demonstrate, the information collected is extremely sensitive and includes information about a user's sexual activity, sex drive, mood, premenstrual systems, and vaginal discharge, among other things:



134. Flo Health entices users to input this information to "stay on top of [their] health," explaining that "[l]ogging symptoms helps Flo detect possible imbalances in your body and advi[s]e you to see a doctor."

135. By encouraging millions of users to provide extensive information about their emotional and physical health, as well as their personal lifestyles and sexual activity, to the Flo App, Flo Health has collected massive volumes of deeply intimate health data about millions of consumers, including Plaintiffs.

136. Despite Flo Health's repeated representations from 2017 to 2019 that it would protect users' intimate private information, Flo Health contracted with numerous third parties, including the Non-Flo Defendants, granting them full access to any information obtained from Flo App users, which the Non-Flo Defendants could use for their own purposes, including advertising and product improvement unrelated to the Flo App.

137. Specifically, Flo Health provided third parties, including the Non-Flo Defendants, with "Standard App Events" and "Custom App Events" created each time users interact with the Flo App. "Standard App Events" are records of routine app functions, such as launching or closing the app, while "Custom Apps Events," are records of user-app interactions unique to the app itself. For example, when a user enters menstruation dates, their weight, sleep cycle, mood, physical or mental symptoms, or any other information in the Flo App, the Flo App registers the user's interaction with that feature as a Custom App Event. Through these Custom App Events, every single interaction within the Flo App is recorded and stored.

138. Flo Health receives and stores a record of all the Custom App Events that occur in the Flo App across its users' devices. Flo Health claims to make use of these records to improve the Flo App's functionality and identify which features are likely to interest new users.

139. Flo Health purposefully designed the Custom App Events of the Flo App to have a descriptive title. For example, when a user enters the week of their pregnancy into the App's calendar, the Flo App 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, the Flo App records the Custom App Event "P_ACCEPT_PUSHES_PERIOD."

140. As early as 2016, Flo Health integrated SDKs into the Flo App. These SDKs were provided by third-party marketing and analytics firms, including the Non-Flo Defendants, and allowed these firms to intercept, receive, and collect the information, which was recorded as users communicated with the Flo App on their devices through these Custom App Events.

141. Because of the way that Flo Health titles the Custom App Events of the Flo App (that is, titling them "R_PREGNANCY_WEEK_CHOSEN" rather than something generic, like "Event 1"), the Custom App Events convey intimate details about a users' health, including their menstruations, fertility, or pregnancies. For example, if a user, through their interactions with the Flo App, indicates a date in the pregnancy calendar, that data is collected, transmitted, and disclosed to the Non-Flo Defendants by Flo Health without the user's authorization or consent. The Non-Flo Defendants can then access and use this information for any purpose, including marketing and analytics. The same goes for when a user removes dates from the pregnancy calendar, indicating that the user's pregnancy was either voluntarily or involuntarily terminated.

142. By including intimate health information in the title of the Custom App Events, Flo Health, without consent or authorization, transmitted, and disclosed Flo App users' communications of private intimate health information with the Non-Flo Defendants. This directly contradicts Flo Health's statements in its privacy policies that it would not disclose this information.

143. Despite assurances made to consumers, Flo Health spent years feeding the intimate and protected health information of millions of users to the Non-Flo Defendants through the SDKs to use in any manner whatsoever, in the form of Custom App Events. For example, Flo Health disclosed Custom App Event information to:

a. Facebook from at least June 2016 to February 2019;

b. Flurry from at least June 2016 to February 2019;

c. Google's subsidiary Fabric from at least November 2016 to February 2019;

d. AppsFlyer from at least May 2018 to February 2019; and

e. Google from at least September 2018 to February 2019.[20]

144. Plaintiffs confirmed that Flo Health shared data with a majority of these Non-Flo Defendants by analyzing Internet traffic sent to and from the Flo App.

145. Plaintiffs conducted this analysis by launching a version of the Flo App that was available during September 2018 and monitoring which servers the App established a connection with over the Internet. Plaintiffs' analysis revealed that the Flo App established connections with at least the following:

| Non-Flo Defendant | URL |
|---|---|
| Facebook | facebook.com |
| AppsFlyer | t.appsflyer.com |
| Flurry | data.flurry.com<br>proton.flurry.com |
| Google | issuetracker.google.com<br>play.google.com<br>googleapi.com |
| Fabric | flo-health.firebaseio.com |

146. Next, Plaintiffs monitored data entering and leaving the September 2018 version of the Flo App while performing basic functions, such as updating period days from the prior month, or updating daily symptoms. In response to these user actions, the Flo App transmitted data to at least the following Non-Flo Defendants:

| Non-Flo Defendant | URL |
|---|---|
| Facebook | graph.facebook.com |
| AppsFlyer | events.appsflyer.com<br>t.appsflyer.com |
| Flurry | data.flurry.com |

[20] Complaint, *In the Matter of Flo Health Inc.*, FEDERAL TRADE COMMISSION, No. 1923133, https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf.

147. Flo Health also sent data to the Non-Flo Defendants even when users ***were not interacting*** with its App. An analysis of data sent and received by the same 2018 version of the Flo App showed that, absent any interaction, data was being sent to at least Facebook (at graph.facebook.com) and Flurry (at data.flurry.com).

148. Notably, Plaintiffs' analysis is merely preliminary and does not represent the full extent of Flo Health's misconduct and the misconduct that flowed from there. For instance, while not depicted in Plaintiffs' analysis, the FTC has independently confirmed that Flo Health also sent data to Google between at least September 2018 and February 2019.[21]

149. Despite Flo Health's assurances, the Non-Flo Defendants were free to use Plaintiffs' and Class members' intimate health data for ***any*** purpose. Indeed, Facebook, Google, and Flurry each maintain an extensive marketing and advertising practice. Significantly, the FTC independently found that Non-Flo Defendant Facebook use Flo App event data "for its own purposes, including its own research and development purposes."[22] As discussed in ¶ 128 and fn.19, this data allows Non-Flo Defendants to target Plaintiffs and Class members for their own purposes, including advertisements and marketing campaigns to boost their own revenue.

150. Significantly, Flo Heath appears to have removed at least some of the Non-Flo Defendants' SDKs more recent versions of the Flo App. Plaintiffs conducted the same analysis described above, using a version of the Flo App from April 2021—after Flo Health reached a settlement with the FTC for ***sharing highly sensitive user data with Facebook*** (*see* ¶¶217-232), and after it was severely criticized by the NYSFDS (*see* ¶¶233-240)**.** Unlike the September 2018 version of the Flo App, the April 2021 version did not appear to establish a connection with (or transmit data to) a Facebook or Flurry server. However, it still maintained connections to servers operated by Non-Flo Defendants Google, AppsFlyer, and Fabric.

---

[21] Complaint, *In the Matter of Flo Health Inc.*, FEDERAL TRADE COMMISSION, No. 1923133, https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf.

[22] *Id.*

151. Defendants also tracked users' behavior while using the app by obtaining critical pieces of data from the mobile devices, including "persistent identifiers." These identifiers are a set of unique data points (typically numbers and letters), akin to a social security number, that can link one specific individual to all the apps on her device and her activity on those apps, allowing her to be tracked over time and across devices (e.g., smart phones, tablets, laptops, desktops and smart TVs).

152. When a user is engaged in the Flo App every action on the device the user is using is linked to a unique and persistent identifier that constructs a profile of the user on that mobile device. These identifying numbers are unique to each device and put in place by app developers so that their SDK partners can collect the users' personal information and build an immense online profile across all the devices they use. Their app usage, geographic location (including likely domicile), and internet navigation all help to build a personal profile.

153. The common persistent identifiers for Apple are the ID for Advertisers ("IDFA") and ID for Vendors ("IDFV"). Both the IDFA and the IDFV are unique, alphanumeric strings that are used to identify an individual device—and the individual who uses that device—in order to track and profile the user, and to serve her with targeted advertising.

154. The common persistent identifiers in the Android operating system are the Android Advertising ID ("AAID") and the Android ID. The AAID and Android ID are unique, alphanumeric strings assigned to a user's device and used by apps and third parties to track and profile the user, and to serve her targeted advertising.

155. Additional persistent identifiers include data about a specific device, including details about its hardware—such as the device's brand (e.g., Apple or Android), the type of device (e.g., iPhone, Galaxy, iPad)—and details about its software, such as its operating system (e.g., iOS or Android). This data can also include more detailed information, such as the network carriers (e.g., Sprint, T-Mobile, AT&T), whether it is connected to Wi-Fi, and the "name" of the device. The name of the device is often particularly personal, as the default device name is frequently configured to include user's first and/or last names. In combination, the pieces of data provide a level of detail

about the given device that allows that device and its user to be identified individually, uniquely, and persistently.

156. The Center for Digital Democracy, and the FTC described how and why a persistent identifier alone facilitates behavioral advertising:

> With the increasing use of new tracking and targeting techniques, any meaningful distinctions between personal and so-called non-personal information have disappeared. This is particularly the case with the proliferation of personal digital devices such as smart phones and Internet-enabled game consoles, which are increasingly associated with individual users, rather than families. This means that marketers do not need to know the name, address, or email of a user in order to identify, target and contact that particular individual.[23]

157. A 2014 report by the Senate Committee on Homeland Security and Governmental Affairs entitled "Online Advertising and Hidden Hazards to Consumer Security and Data Privacy" amplifies this concern in light of the growth of third-party trackers that operate behind the scenes in routine online traffic:

> Although consumers are becoming increasingly vigilant about safeguarding the information they share on the Internet, many are less informed about the plethora of information created about them by online companies as they travel the Internet. A consumer may be aware, for example, that a search engine provider may use the search terms the consumer enters in order to select an advertisement targeted to his interests. Consumers are less aware, however, of the true scale of the data being collected about their online activity. A visit to an online news site may trigger interactions with hundreds of other parties that may be collecting information on the consumer as he travels the web. The Subcommittee found, for example, a trip to a popular tabloid news website triggered a user interaction with some 352 other web servers as well.…The sheer volume of such activity

[23] *See* Comments of The Center for Digital Democracy, et al., FTC, *In the Matter of Children's Online Privacy Protection Rule*, at 13-14 (Dec. 23, 2011), https://www.ftc.gov/sites/default/files/documents/public_comments/district-columbia-00373%C2%A0/00373-82399.pdf.

> makes it difficult for even the most vigilant consumer to control the data being collected or protect against its malicious use.[24]

158. While disclosing a user's personal data to select and serve an advertisement (or to conduct any third-party analytics or otherwise monetize user data), Defendants pass identifying user data to an ever-increasing host of third parties, who, in turn, may pass along that same data to their affiliates. Each entity may use that data to track users over time and across the Internet, on a multitude of increasingly complex online pathways, with the shared goal of targeting users with advertisements.

159. The ability to serve targeted advertisements to (or to otherwise profile) a specific user no longer turns upon obtaining the kinds of data with which most consumers are familiar (name, email addresses, etc.), but instead on the surreptitious collection of persistent identifiers, which are used in conjunction with other data points to build robust online profiles. These persistent identifiers are better tracking tools than traditional identifiers because they are unique to each individual, making them more akin to a social security number. Once a persistent identifier is sent "into the marketplace" it is exposed to—and thereafter may be collected and used by—an almost innumerable set of third parties.

160. In sum, personal information is collected by Defendants, which is then sold to third parties who track and use the collected information and analyze it with sophisticated algorithms to create a user profile. This profile is then used to serve behavioral advertising to individuals whose profile fits a set of demographic and behavioral traits.

---

[24] Staff Report, *Online Advertising and Hidden Hazards to Consumer Security and Data Privacy*, Permanent Subcommittee on Investigations of the U.S. Senate Homeland Security and Governmental Affairs Committee (May 15, 2014), at 1, available at https://www.hsgac.senate.gov/imo/media/doc/REPORT%20-%20Online%20Advertising%20&%20Hidden%20Hazards%20to%20Consumer%20Security%20&%20Date%20Privacy%20(May%2015%202014)2.pdf (accessed Sept. 1, 2021).

### C. Defendants' Failure to Obtain User Consent

161. Between 2017 and 2019, Flo Health made repeated representations to Flo App users, promising that it would keep intimate health data they entered into the App private, and that Flo Health would only use Flo App users' data in order to provide and improve Flo App's services.

162. Based on Flo Health's representations and the guarantees made in the company's Privacy Policy, millions of users entrusted Flo Health with intimate information regarding their physical and mental health, romantic relationships, sex life, and lifestyle preferences.

163. Flo Health's Privacy Policy assures customers that "[w]hen you use Flo, you are trusting us with intimate personal information. We are committed to keeping that trust, which is why our policy as a company is to take every step to ensure that individual user's data and privacy rights are protected . . . ."[25]

164. More specifically, the Flo Health Privacy Policy, effective between August 28, 2017 and February 19, 2019, stated that Flo Health "may share certain" personal data with third parties, but only "information that is reasonably necessary to perform their work" which involves "supply[ing] software applications, web hosting, and other technologies for the App."[26]

165. The same Flo Health Privacy Policy stated that any information shared with third parties "**exclud[ed] information regarding your marked cycles, pregnancy, symptoms**, notes and other information that is entered by you and that you do not elect to share." (emphasis added).[27]

166. The same Flo Health Privacy Policy stated that third parties could not use Flo App users' personal information "for any other purpose except to provide services in connection with the App."[28]

---

[25] *Privacy Policy*, FLO HEALTH, INC. (effective Oct. 24, 2020), https://flo.health/privacy-policy.

[26] *Privacy Policy*, FLO HEALTH, INC. (effective Aug. 28, 2017), https://flo.health/privacy-policy-archived/aug-28-2017.

[27] *Id.*

[28] *Id.*

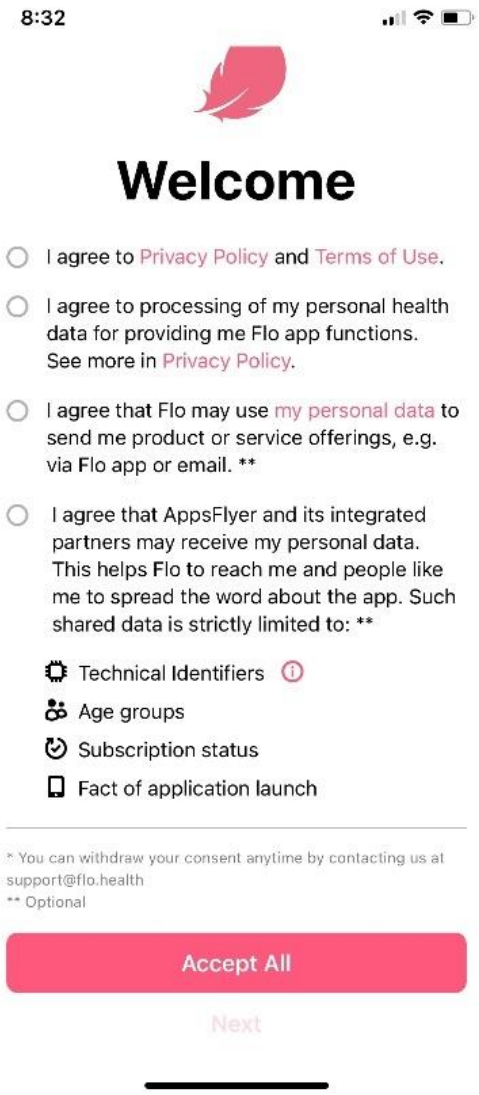
167. Furthermore, later versions of the Flo Health Privacy Policy, effective between May 25, 2018 and February 19, 2019, specifically stated that Flo Health would not disclose "any data related to health" to either of the mobile analytics firms AppsFlyer or Flurry:[29]

a. "AppsFlyer is a mobile marketing platform. We may share certain non-identifiable information about you and some Personal Data **(but never any data related to health)** in order to carry out marketing activities and provide you better and more targeted, tailor-made service." (emphasis added).

b. "We may share certain non-identifiable information about you and some Personal Data **(but never any data related to health)** with Flurry."

168. Consistent with the assurances made in the Flo Health Privacy Policy, new users of the Flo App receive a notification, informing them that personal data disclosed to AppsFlyer is "strictly limited" to technical identifiers, age groups, subscription status, and data indicating that the App has been opened by the user:

[29] *Privacy Policy*, FLO HEALTH, INC. (effective May 25, 2018) (emphasis added), https://flo.health/privacy-policy-archived/may-25-2018.




169. Moreover, analysis of the above screenshot demonstrates how deceptive Flo Health's purported disclosures really were. A reasonable Flo Health user would have assumed that to continue to use the Flo Health App, they must click on the "Accept All" button that is prominently featured on the bottom of the screen in a bright, pink color.

170. Significantly, and upon closer inspection, one sees that there are two provisions of the Privacy Policy that are much more hidden and in a greyed-out color—which blends into the white background. One of those provisions indicates that the term that the user is reading is "Optional."

171. The only way a user would know this is if she was able to read, on a small cellphone or other personal device screen, and understand that the two asterisks next to some of the individual Terms are linked to the footnote at the bottom that indicates "Optional."

172. One such Term states that "I agree that AppsFlyer and its integrated partners may receive my personal data. This helps Flo to reach me and people like me to spread the word about the app. Such shared data is strictly limited to: Technical identifiers; Age groups; Subscription status; [and] Fact of application launch."

173. Another such Term states "I agree that Flo may use my personal data to send me product or service offerings, e.g. via Flo app or email."

174. In other words, a user ***does not have to click on the Terms*** discussed in ¶¶172-73 in order to continue to use the App. A user can individually click on the first two Terms listed on the screenshot above and continue on.

175. However, because Flo Health purposely hides this fact through the use of small-text and grey-font in a white background, while simultaneously featuring the "Accept All" button in a highlighted color in a more prominent fashion, Flo Health purposefully and intentionally seeks to deceive its users and causes them to give consent to the optional Terms, including the Terms discussed in ¶¶172-73, when they may not otherwise would have.

176. Even if a user consented to the Terms discussed in ¶172, the user only consented to the sharing of data for the "***strictly limited***" purposes that were outlined in that Term.

177. Similarly, Flo Health's Privacy Policy made similar assurances about the "strictly limited" nature of the sharing of data to Facebook, Google, and Google's subsidiary Fabric. The Privacy Policy stated that these third parties would ***only*** receive "non-personally identifiable information," "[p]ersonal Data like device identifiers," or "device identifiers." The Privacy Policy did not indicate that these third parties would receive access to any record of the Custom App Events (containing intimate health data) registered by the Flo App, or advertising identifiers.[30]

[30] *Id.*

178. Specifically, the Flo Privacy Policy stated as follows:

a. "We use Facebook Analytics and Google Analytics tools to track installs of our App. Normally, Facebook and Google collect **only non-personally identifiable information,** though some **Personal Data like device identifiers** may be transferred to Facebook ...." (emphasis added).

b. "**Fabric may use device identifiers** that are stored on your mobile device and allow us to analyze your use of the App in order to improve our app feature [sic]." (emphasis added).

179. By disclosing Custom App Events that users generated through their communications of intimate health data with the Flo App, Flo Health consistently violated these terms of its Privacy Policy.[31]

180. Flo Health further violated the guarantees made in its Privacy Policy by agreeing to contractual terms that directly contradicted its Privacy Policy. When entering into contracts with numerous third parties—including Defendants Facebook, Google, AppsFlyer, and Google subsidiary Fabric—Flo Health agreed to boilerplate terms of service which permitted these third parties to use any user information communicated with, and obtained from Flo App users for the Non-Flo Defendants' own purposes, including purposes explicitly excluded by the Flo Privacy Policy, such as advertising, marketing, research, and development:

a. Facebook's Business Tools Terms stated: "We use [aggregated] Event Data to personalize the features and content (including ads and recommendations) we show people on and off our Facebook Company Products .... We may also use Event Data ... for research and development purposes, and to ... improve the Facebook Company Products." That "Event Data" includes Custom App Events.

b. Google Analytics's Terms of Service stated: "Google and its wholly owned subsidiaries may retain and use ... information collected in [Flo Health's] use of the Service."

[31] *See, e.g.*, Sam Schechner and Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL ST. J. (Feb. 22, 2019 11:07 AM ET), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636 (detailing how "Facebook software inside Flo records that action and send a 'custom app event' to Facebook. It includes data about the user's device as well as other data Flo defines, such as the fact that the user may be ovulating.").

c. AppsFlyer's Terms of Use stated: "You hereby allow AppsFlyer to collect, store, use and process Customer Data," where "Customer Data" was defined to include "data concerning the characteristics and activities" of app users.

d. The Fabric Software and Services Agreement stated: "[Flo Health] acknowledges and agrees that Google [Fabric] may use Usage Data for its own business purposes," where "Usage Data" was defined to mean "all information, data and other content, not including any [identifying data], received by Google related to [Flo Health]'s use of the Fabric Technology…."[32]

181. Indeed, the FTC independently found that at least one Non-Flo Defendant—i.e., Facebook—used Flo App Custom Event data for its own research and development purposes.[33]

182. As a result of these agreements, the Non-Flo Defendants were able to use intimate health data about users, including whether they were pregnant, attempting to get pregnant, or menstruating, for their own purposes, including to boost the Non-Flo Defendants' own revenue by targeting Plaintiffs and Class members for advertisements and marketing campaigns.

183. Because Flo Health failed to disclose the full extent of its data practices, Plaintiffs and Class members were not able to consent to the Non-Flo Defendants' use of their intimate health data.

184. Following publication of the *Wall Street Journal* report exposing Flo Health's privacy violations, Flo Health received several hundred complaints from Flo App users about the unauthorized disclosures of health information to Facebook. For example, users stated:

a. "I'm absolutely disgusted at this invasion of my most personal information."

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 party?"

---

[32] Complaint, *In the Matter of Flo Health Inc.*, FEDERAL TRADE COMMISSION, No. 1923133, https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf.

[33] *Id.*

185. Alice Berg, a 25-year-old student, told the *Wall Street Journal* "I think it's incredibly dishonest of them that they're just lying to their users especially when it comes to something so sensitive."[34]

186. Additionally, following the *Wall Street Journal* publication, more than 100 Flo App users asked Flo Health to delete their accounts and/or data or told Flo Health they were deleting, or would be deleting, the Flo App.

### D. Plaintiffs and Class Members Have a Reasonable Expectation of Privacy, Especially With Respect to the Intimate Health Data That Users Shared Here

187. Plaintiffs and Class members have a reasonable expectation of privacy in their intimate health data, which Flo Health collected, stored, and disclosed to third parties, including the Non-Flo Defendants. Violation of this expectation of privacy harms users of the Flo App (i.e., Plaintiffs and the Class).

188. Several studies examining the collection and disclosure of consumers' intimate personal data confirm that the disclosure of intimate personal data from millions of individuals, as Defendants have done here, violates expectations of privacy that have been established as general social norms.

189. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' personal data.

190. For example, a recent study by *Consumer Reports* shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about

[34] Sam Schechner and Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL STREET JOURNAL, (Feb. 22, 2019 11:07 AM), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

them.[35] Moreover, according to a study by *Pew Research Center*, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[36]

191. Users act consistently with these preferences. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to share data when prompted.[37]

192. In addition, three bioethics and health law professors at Johns Hopkins University, the University of Pittsburgh, and Wake Forest University School of Law recently published a paper that explored the ethical concerns associated with the monetization of menstruation app data—i.e., the conduct at issue here. The paper noted that given this sort of data's "intimate nature, users expected greater privacy and respect" and also explained that because this data was solicited by for-profit apps and shared with other for-profit companies, the privacy concerns are even more acute: "[menstrual cycle details and other intimate health data are] solicited by the apps, processed by Facebook-owned algorithms and converted into targeted advertisements. The potential for the triangulation of intersecting datasets heightens the threat and perceived harms of privacy violation."[38]

193. The paper expands further on the unique privacy concerns with monetizing this intimate health data: "[M]any users assume that the data they enter are protected by existing privacy

---

[35] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

[36] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER, (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[37] Margaret Taylor, *How Apple screwed Facebook*, WIRED, (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

[38] Marielle S. Gross, Amelia Hood, Bethany Corbin, *Pay No Attention to that Man behind the Curtain: An Ethical Analysis of the Monetization of Menstruation App Data* (Nov. 2020), available at https://www.researchgate.net/publication/345392497_Pay_No_Attention_to_that_Man_behind_the_Curtain_An_Ethical_Analysis_of_the_Monetization_of_Menstruation_App_Data.

regulations that apply to similarly sensitive data. The apps' user interface capitalizes on the illusion of privacy of data contained on a handheld personal device and downplays the third party use of these data for profit. . . . We argue that in the case of menstruation apps, the sale of users' identified data is violating due to the expectations of privacy in relation to the intimacy of the data. . . . Unlike other targeted ads, these capitalize on an especially sensitive class of traditionally privileged health data. The resulting experience of advertisements tailored to one's menstrual or pregnancy status is uniquely invasive. Being sold tampons while you are bleeding represents an unprecedented loss of privileged consumer self-knowledge and the power associated. The resulting revelation of consumer preferences increases user vulnerability and helps explain the discomfort felt when users were made aware of this process."[39]

194. The paper further highlights the real-world harm that users of ovulation apps experience when this intimate health data is shared with third-parties (without consent) for advertising purposes: "For example, consider someone using a menstruation app to assist in conception who, after two months, starts receiving advertisements for a local IVF clinic. Attempting to conceive is already correlated with feelings of anxiety; to perceive a suggestion of infertility may worsen those feelings. In turn, anxiety can lower one's chance of conceiving. Such use of advertisements risks psychological harm beyond any harm stemming from the potentially flawed health guidance."[40]

195. The concern about sharing intimate data about women's health and pregnancy efforts is compounded by the reality that advertisers view this type of information as particularly high-value. Indeed, having access to the data women share with apps like the Flo App allows advertisers to obtain data on children before they are even born. As one article put it: "the datafication of family life can begin from the moment in which a parent thinks about having a baby."[41] The article

---

[39] *Id.*

[40] *Id.*

[41] Veronica Barassi, *Tech Companies Are Profiling Us From Before Birth*, THE MIT PRESS READER, https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/.

continues "Children today are the very first generation of citizens to be datafied from before birth, and we cannot foresee — as yet — the social and political consequences of this historical transformation. What is particularly worrying about this process of datafication of children is that companies like Google, Facebook, and Amazon are harnessing and collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles."[42]

196. Other privacy law experts have expressed concerns about the disclosure to third parties of a users' intimate health data. For example, Dena Mendelsohn—the former Senior Policy Counsel at Consumer Reports and current Director of Health Policy and Data Governance at Elektra Labs—explained that having your personal health information disseminated in ways you are unaware of could have serious repercussions, including affecting your ability to obtain life insurance and how much you pay for that coverage, increase the rate you're charged on loans, and leave you vulnerable to workplace discrimination.[43]

197. Mendelsohn, who is quoted in a recent Consumer Reports article highlighting the harms that could arise from the disclosure to third parties of the intimate menstrual health data, notes that "[w]ith issues like pregnancy discrimination still a concern for many women, those using reproductive health apps will want to be sure their private information stays private."[44] Given that "health app makers can collect, buy, and sell your data without your knowing consent," Mendelsohn explains that app developers should use consumers' data only for the purpose of the app and not share or sell the information, and should face strict penalties when they violate their privacy policies—as Flo Health did here.[45]

---

[42] *Id.*

[43] Donna Rosato, *What Your Period Tracker App Knows About You*, CONSUMER REPORTS (Jan. 28, 2020), https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you/.

[44] *Id.*

[45] *Id.*

198. Flo Health purported to act consistently with consumer expectations by promising not to share their intimate health data with third parties and by promising that the limited data that they did share would only be used to provide the Flo App's services.

199. Instead, Flo Health provided the Non-Flo Defendants with the ability and free reign to surreptitiously receive and record even the most personal and protected information communicated by users of the Flo App—all without their authorization or consent.

200. This constitutes a violation of Plaintiffs' and Class members' privacy interests, as demonstrated by the outrage users conveyed when they learned that their intimate health data was disclosed by Flo Health to third parties, including the Non-Flo Defendants. For example, as one user stated: "Why would you EVER think it is ok to share that personal, private information with a third party?"[46]

### E. Plaintiffs' Information that Flo Health Disclosed is Plaintiffs' Property, has Economic Value, and its Illicit Disclosure Caused Economic Harm

201. Companies like Defendants Facebook and Google have built their businesses around the collection of personal data because the "world's most valuable resource is no longer oil, but ***data***."[47] As the *Economist* analogized, a user's personal data is "the oil of the digital era."[48]

202. It is common knowledge in the industry that there is an economic market for consumers' personal data—including the personal health data that Flo Health collected from its users. In fact, this type of data is routinely bought and sold for ***real-world dollars***.

203. In 2013, the *Financial Times* reported that the data-broker industry profits from the trade of thousands of details about individuals, and that within that context, "age, gender, and

---

[46] Complaint, *In the Matter of Flo Health Inc.*, No. 1923133 (F.T.C. June 17, 2021), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf.

[47] *The world's most valuable resource is no longer oil, but data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (emphasis added).

[48] *Id.*

location" information" are sold for about "$0.50 per 1,000 people."[49] This estimate was based upon "industry pricing data viewed by the Financial Times," at the time.[50]

204. In 2015, *TechCrunch* reported that "to obtain a list containing the names of individuals suffering from a particular disease," a market participant would have to spend about "$0.30 per name."[51] That same article noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge"[52] and that the value of a single user's data (within the corporate acquisition context) can vary from $15 to more than $40 per user.[53]

205. In an August 2021 Washington Post article, legal scholar Dina Srinivasan said that consumers "should think of Facebook's cost as [their] data, and scrutinize the power it has to set its own price." And this price is only increasing. According to Facebook's own financial statements, the value of the average American's data in advertising sales rose from $19 per year to $164 per year between 2013 and 2020.[54]

206. The Organization for Economic Cooperation and Development ("OECD") published in 2013 a paper titled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[55] In this paper, the OECD measured prices demanded by companies

---

[49] Emily Steel, et al., *How much is your personal data worth?*, FIN. TIMES (June 12, 2013), https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz3myQiwm6u.

[50] *Id.*

[51] Pauline Glickman and Nicolas Glady, *What's the Value of Your Data?*, TECHCRUNCH (Oct. 13, 2015), https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/.

[52] *Id.*

[53] *Id.*

[54] Geoffrey A. Fowler, *There's no escape from Facebook, even if you don't use it*, THE WASHINGTON POST (Aug. 29, 2021), https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/.

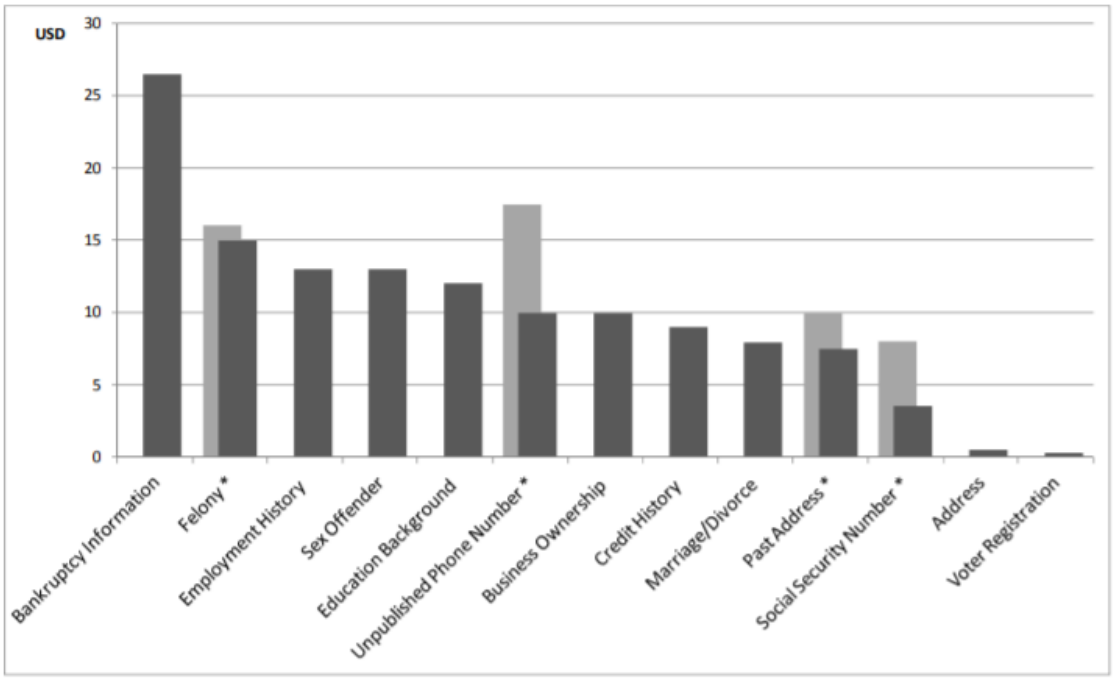
[55] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS, NO. 220 (Apr. 2, 2013), https://www.oecd-ilibrary.org/docserver/5k486qtxldmq-en.pdf?expires=1630429771&id=id&accname=guest&checksum=EE508E4C5722D02DCC45931B4D7B63A0.

concerning user data derived from "various online data warehouses."[56] OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[57]

207. The OECD published in this same paper a chart demonstrating the various "Market prices for personal data by type"[58]:

**Figure 7. Market prices for personal data by type**

(per record)




* two different prices provided by different providers.

*Sources:* Locate Plus (address Unpublished Phone Number Felony) Pallorium (address, past address Unpublished Phone Number Social Security Number) KnowX via Swipe Toolkit (Past address, Marriage/Divorce Bankruptcy Information Business Ownership) LexisNexis via Swipe Toolkit (Education Background Employment History Social Security Number Felony sex offender) Experian (Credit History) Voters online.com (voter registration)

[56] *Id.* at 25.

[57] *Id.*

[58] *Id.* at 26.

208. Notably, the value of personal data also fluctuates based upon demographics, race, and background, as analyzed in a 2020 study by *MacKeeper* and YouGov (an international research and data-analytics firm).[59] As reported by *Invisibly* on July 13, 2021, the study showed that "personal data for 18-24-year-olds is notably higher than any other demographic, while businesses have shown a willingness to pay significant amounts for personal data from Black and Middle Eastern audiences," and that "[b]ecause there are more females on the planet than males, male data tends to come at a slightly higher premium."[60] The study published the following information:

| Demographic | | Cost for Data Per Person | Percentage of Population |
|---|---|---|---|
| Sex Assignment | Male | $0.15 | 48.59% |
| | Female | $0.14 | 51.41% |
| Age | Age 18-24 | $0.36 | 11.92% |
| | Age 55+ | $0.05 | 32.33% |
| Ethnicity | Middle Eastern | $0.62 | 1.21% |
| | Hispanic | $0.01 | 8.09% |
| Family Annual Income | $40,000-$49,999 | $0.02 | 4.94% |
| | $120,000-$149,999 | $0.33 | 1.84% |

209. There is also a twin-market for users' data in the dark web. "As of May 2021, you can buy access to a hacked Facebook account on the dark web for $65 (or its crypto equivalent), an entire US voter database for $100, and even a hacked Coinbase verified account for $610."[61]

210. Notably, *Invisibly* reported that personal medical information is one of the ***most valuable pieces of data*** within this data-market. "It's worth acknowledging that because health care

[59] Ruslana Lishchuk, *Most Desired Data: Whose is the most in demand, and how much is it worth*?, MACKEEPER (Nov. 16, 2020), https://mackeeper.com/blog/most-desired-data/.

[60] *How Much is Your Data Worth? The Complete Breakdown for 2021*, INVISIBLY (July 13, 2021), https://www.invisibly.com/learn-blog/how-much-is-data-worth.

[61] *Id.*

records often feature a more complete collection of the patient's identity, background, and personal identifying information (PII), health care records have proven to be of particular value for data thieves. While a single social security number might go for $0.53, a complete health care record sells for $250 on average. For criminals, the more complete a dataset, the more potential value they can get out of it. As a result, health care breaches increased by 55% in 2020."[62] The article noted the following breakdown in average price for record type:

| Record Type | Average Price |
|---|---|
| Health Care Record | $250.15 |
| Payment Card Details | $5.40 |
| Banking Records | $4.12 |
| Access Credentials | $0.95 |
| Social Security Number | $0.53 |
| Credit Record | $0.31 |
| Basic PII | $0.03 |

211. Furthermore, individuals can sell or monetize their own data, if they so choose. Indeed, ***Defendants*** themselves have valued individuals' personal data in real-world dollars.

[62] *Id.*

212. Facebook has offered to pay individuals for their voice recordings,[63] and has paid teenagers and adults up to $20 a month plus referral fees to install an app that allows Facebook to collect data on how individuals use their smartphones.[64]

213. Google has offered a similar program, where Google's "ScreenWise Meter" allowed Google to see anything that the users see on their phone screen and web browser window (including every single action a user makes on any website), and also allowed Google to monitor all the user's app usage and network traffic.[65] In exchange for this data, Google offered $20 a month.[66] The "Ipsos Screenwise" program, which is currently run by Google and for Google, also exchanges money for personal data.[67] Through the Ipsos Screenwise program, users can earn $16 per month to sell their internet usage and browser habits data.[68]

214. A myriad of other companies and apps such as Nielsen Data, Killi, DataCoup, and AppOptix offer consumers money in exchange for their personal data.[69]

215. The personal health data that Flo Health users entered into the App is thus of extraordinary value to companies, including Defendants Google, Facebook, AppsFlyer, and Flurry, because entities in possession of such data can learn a panoply of information from a user including:

---

[63] Jay Peters, *Facebook will now pay you for your voice recordings*, THE VERGE (Feb. 20, 2020), https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-prounnciations-app.

[64] Saheli Roy Choudhury and Ryan Browne, *Facebook pays teens to install an app that could collect all kinds of data*, CNBC (Jan. 29. 2019), https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html.

[65] Sydney Li and Jason Kelley, *Google Screenwise: An Unwise Trade of All Your Privacy for Cash*, ELEC. FRONTIER FOUND. (Feb. 1, 2019), https://www.eff.org/deeplinks/2019/02/google-screenwise-unwise-trade-all-your-privacy-cash.

[66] *Id.*

[67] Sam Hawrylack, *Apps that Pay You for Data Collection*, CREDITDONKEY (June 12, 2021), https://www.creditdonkey.com/best-apps-data-collection.html.

[68] *Id.*; *see also Policies and Legal*, IPSOS SCREENWISE PANEL, https://screenwisepanel.com/policies-legal.

[69] *28 Apps That Pay You For Data Collection: Earn a Passive Income*, DOLLAR BREAK (Aug. 12, 2021), https://www.dollarbreak.com/apps-that-pay-you-for-data-collection/.

(1) the menstrual and period cycles of the user; (2) the sexual and masturbation history of the user; (3) whether the user is pregnant or planning on getting pregnant; (4) the bodily or physical symptoms a user is experiencing; (5) the day-to-day behaviors of the user; and much, much more.

216. Given the monetary values that data companies—***including Defendants Google and Facebook***—have ***already*** paid for personal information in the past, Defendants have deprived Plaintiffs of the economic value of their personal health information by acquiring such data without providing proper consideration for Plaintiffs' property.

### F. The FTC Has Filed Suit and Entered Into a Settlement Based on Flo Health's Privacy Violations

217. In response to the *Wall Street Journal's* February 2019 article revealing Flo Health's invasive data sharing practices, the Federal Trade Commission ("FTC") launched an investigation into Flo Health's potential violation of state, federal, and international privacy laws.

218. In January 2021, the FTC filed a complaint against Flo Health, which is incorporated herein by reference. The FTC stated that its investigation revealed that Flo Health disclosed the intimate health information of millions of Flo App users to the Non-Flo Defendants, such as Facebook, Google, Fabric, AppsFlyer, and Flurry.

219. The FTC's investigation further determined that Flo Health conveyed intimate health data in the form of Custom App Events to third parties between at least 2016 and 2019.

220. Based on the findings of its investigation, the FTC determined that Flo Health had violated the privacy of Flo App users in several ways, including by:

a. Flo Health represented that it would not disclose "information regarding … marked cycles, pregnancy, symptoms, notes …" to any third parties, or disclose "any data related to health" to particular third parties. In fact, Flo Health disclosed Custom App events—records of individual users' interactions with various features of the App, which conveyed identifying information about App users' menstrual cycles, fertility, and pregnancies—to various third-party marketing and analytics firms, including the Non-Flo Defendants;

b. Flo Health represented that it would only disclose device identifiers or personal data "like" device identifiers to certain third parties. In fact, in addition to disclosing device and advertising identifiers, Flo Health also disclosed Custom App events conveying health information to those parties;

c. Flo Health represented that third parties would not use Flo App users' personal information "for any other purpose except to provide services in connection with the App." In fact, Flo Health agreed to terms with multiple third parties, including the Non-Flo Defendants, that permitted these third parties to use Flo App users' personal health information for the third parties' own purposes, including for advertising and product improvement. Indeed, from June 2016 to February 2019, Defendant Facebook used Flo App users' personal health data; and

d. Flo Health misrepresented compliance with the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfers, and Data Integrity and Purpose Limitation. Specifically, Flo Health (a) represented compliance with the Privacy Shield frameworks, when in fact it did not give Flo App users notice about to whom their data would be disclosed and for what purposes; (b) disclosed this information without providing Flo App users with a choice with respect to these disclosures or the purposes for which the data could be processed (e.g., Facebook's advertising); (c) failed to limit by contract the third parties' use of users' health data or require by contract the third parties' compliance with the Privacy Shield principles; and (d) processed users' health data in a manner incompatible with the purposes for which it had been collected because Flo Health disclosed the data to third parties under contracts permitting them to use the data for their own purposes.

221. Flo Health entered into a settlement with the FTC over its alleged privacy violations on January 13, 2021.

222. The proposed settlement would require Flo Health to obtain an independent review of its privacy practices and obtain the consent of app users before making further disclosures of their health information.

223. The proposed settlement would also prohibit Flo Health from further misrepresenting (1) the purposes for which Flo Health or entities to whom it discloses data collect, maintain, use, or disclose the data; (2) the extent to which consumers may exercise control over Flo Health's access, collection, maintenance, use, disclosure, or deletion of such data; (3) Flo Health's compliance with any privacy, security, or compliance program; and (4) the extent to which Flo Health collects, maintains, uses, discloses, deletes, or protects users' personal information. In addition, Flo Health must notify affected users about the disclosure of their personal information and instruct any third party that received users' health information to destroy that data.

224. The FTC voted 5-0 to accept the proposed administrative complaint and the consent agreement with Flo Health. However, certain Federal Trade Commissioners believed that the proposed settlement did not go far enough. Specifically, Commissioners Rohit Chopra and Rebecca Kelly Slaughter concurred in part and dissented in part from the proposed settlement, and (in a January 13, 2021 statement) expressed "disappoint[ment] that the [FTC] is not using all of its tools to hold accountable those who abuse and misuse personal data," such as alleging Flo Health's violation of the FTC's Health Breach Notification Rule—which requires "vendors of unsecured health information, including mobile health apps, to notify users and the FTC if there has been an unauthorized disclosure."[70]

225. Commissioners Chopra and Slaughter stated further: "In our view, the FTC should have charged Flo with violating the Health Breach Notification Rule. Under the rule, Flo was obligated to notify its users after it allegedly shared their health information with Facebook, Google, and others without their authorization. Flo did not do so, making the company liable under the rule."

[70] Joint Statement of Commissioner Rohit Chopra and Commissioner Rebecca Kelly Slaughter Concurring in Part, Dissenting in Part, *In the Matter of Flo Health, Inc.*, Commission File No. 1923133 (F.T.C. Jan. 13, 2021), https://www.ftc.gov/system/files/documents/public_statements/1586018/20210112_final_joint_rcrks_statement_on_flo.pdf.

Enforcing this rule, they explained, "may induce firms to take greater care in collecting and monetizing our most sensitive information."[71]

226. On January 28, 2021, the FTC published the proposed consent agreement for public comment, requiring comments by March 1, 2021.

227. The FTC received five comments, which raised issues including (1) that the complaint should have alleged that Flo Health violated the FTC's Health Breach Notification Rule; (2) concern that the mechanism by which the Flo App obtains consent for third-party disclosures is inadequate; (3) concern over the failure to provide redress for injured consumers; (4) concern that Facebook will not delete the data received from Flo Health; and (5) concern that highly sensitive personal information was sold in violation of the Health Information Portability and Accountability Act.[72]

228. One such comment was submitted by the World Privacy Forum ("WPF")—a non-profit public interest research group focused on privacy issues, including health privacy. The WPF's comments raised its concerns "about the FTC's decision to not require notification in regards to the FTC Health Breach Notification Rule."[73] Specifically, the WPF suggested that Flo Health's activities may have narrowly qualified as falling under the FTC's Health Breach Notification Rule because Flo Health allowed Flo App users to import Flo Health Data to vendors of personal health records ("PHRs"), such as Fitbit—and that the Flo App had specific settings by which users could connect the Flo App to Fitbit. On this basis, the WPF recommended that the FTC take a closer look to see if Flo Health's conduct warranted notification via the Health Breach Notification Rule.[74]

---

[71] *Id.*

[72] Letters from FTC in response to comments regarding proposed consent agreement (June 17, 2021), https://www.ftc.gov/system/files/documents/cases/192_3133_-_flo_health_inc._-_comment_response_letters.pdf.

[73] Comments of the World Privacy Forum to the Federal Trade Commission regarding Proposed Consent Order, *In the Matter of Flo Health, Inc.*, File No. 1923133 (Mar. 1, 2021), https://www.worldprivacyforum.org/wp-content/uploads/2021/03/WPF_Comments_FloHealth_1March2021_fs.pdf.

[74] *Id.*

229. The WPF's comment also raised the following additional concern:

> In researching the Flo app, our experience with the app was that even though some sharing, such as the AppsFlyer sharing, was stated as optional, it did not appear to be possible to avoid consenting at the time of notification. In order to opt out of the consent, users are told that "*You can withdraw your consent anytime by contacting us at support@flo.health."
>
> The FTC has recommended a variety of mobile notice best practices in its report, *Mobile Privacy Disclosures*. (https://www.ftc.gov/news-events/press-releases/2013/02/ftc-staff-report-recommends-ways-improve-mobile-privacy). In this report, the FTC recommended "just in time" disclosures and obtaining affirmative express consent before allowing apps to access sensitive content. We support the idea of just in time disclosures and consent for mobile privacy notifications, and in line with the FTC's report, we think it would be a good practice to allow consumers to be notified about the AppsFlyer sharing ***and*** have the ability to decline consent for that sharing on the very same screen at that time, instead of directing consumers to write an email to support personnel after the fact to request an opt out.[75]

230. On June 22, 2021, the Commission voted 4-0-1 to finalize the settlement, formally issuing a Decision & Order requiring Flo Health to comply with the consent agreement, including by: prohibiting misrepresentations about information privacy; seeking the deletion of data it improperly shared with third parties; obtaining users' affirmative express consent before sharing their health information with third parties; reporting to the FTC future unauthorized disclosures; and obtaining an outside assessment of its privacy practices.

231. In addition, the Decision & Order required Flo Health to provide notice to Flo App users that data about their period and pregnancy had been shared with third parties, including the Non-Flo Defendants.

232. On or about July 5 - July 6, 2021, Flo Health sent the following notice to Flo App users (and also made it available on its website):

> Dear Flo User,
>
> Between June 30, 2016, and February 23, 2019, the company that makes the Flo Period & Ovulation Tracker app sent an identifying number related to you and

[75] *Id.* (emphasis in original).

> information about your period and pregnancy to companies that help us measure and analyze trends, usage, and activities on the app, including the analytics divisions of Facebook, Flurry, Fabric, and Google. No information was shared with the social media divisions of these companies. We did not share your name, address, or birthday with anyone at any time.
>
> We do not currently, and will not, share any information about your health with any company unless we get your permission. We recently entered into a settlement with the Federal Trade Commission, the nation's consumer protection agency, to resolve allegations that sharing this information was inconsistent with the promises we made to you. Learn more about the settlement at https://www.ftc.gov/enforcement/cases-proceedings/1923133/flo-health-inc. This page also includes links to resources for consumers to help them evaluate the risks and benefits of sharing information with health apps.

### G. The NYSDFS Found That Facebook Received Sensitive Health Information From the Flo App

233. At the direction of New York Governor Andrew M. Cuomo and following the *Wall Street Journal* publication, the NYSDFS opened an investigation into Facebook Payments, Inc., a subsidiary of Facebook, regarding the "outrageous abuse of privacy" resulting from data collection practices that included the collection of intimate health data from Flo Heath users.

234. NYSDFS investigated Facebook's data collection practices, finding that the company had received "Custom App Events" through its agreement with Flo Health, among other apps, despite Facebook's policy not to do so. Indeed, according to the NYSDFS report, Facebook's applicable terms prohibit app developers and other third parties from sending Facebook sensitive data, such as health-related data. Specifically, the terms state: "You [i.e., app developer] will not share Customer Data with us that you know or reasonably should know . . . includes health, financial information, or other categories of sensitive information (including any information defined as sensitive under applicable law)."

235. Despite this policy, the NYSDFS report notes that it is "clear that Facebook's internal controls on this issue have been very limited and were not effective at enforcing Facebook's policy or preventing the receipt of sensitive data"—and further that Facebook "does little to ensure that developers are actually aware of this prohibition or to make particular note of it when the developers create the Customer Events that result in the transmission of sensitive data"—i.e., which is precisely

at issue here, given the highly descriptive Custom App Events Flo Health shared with the Non-Flo Defendants, including Facebook.

236. Importantly, the NYSDFS also explained that while Facebook "acknowledge[d] the problem—i.e., that in the past it did receive sensitive information from app developers contrary to its own policy—it has failed to provide sufficient detail about, among other things, specifically what kinds of sensitive information was obtained, how regularly it was received, or which app developers violated the rules by transmitting such information."

237. As a result of Facebook's receipt of "Custom App Events" through its agreement with Flo Health, and Facebook's failure to enforce its own policy, Facebook received, stored, and analyzed users' intimate health data. This data was then used for research and development purposes at Facebook, including providing personalized content and advertisements.

238. The NYSDFS noted several deficiencies and remediation efforts that Facebook could undertake, including efforts to ensure intimate health data is not conveyed to Facebook, and concluded that until there are real ramifications for violating Facebook's policies, Facebook will not be able to "effectively prohibit the sharing of sensitive user data with third-parties."

239. Further, Facebook was unwilling to conduct a review of the data it collected, including intimate health data from Flo App users. Since Facebook has refused to audit its own systems, Facebook continue to retain users' intimate health data and has not destroyed it. The NYSDFS called on federal regulators to compel Facebook to conduct a review.

240. The NYSDFS also explained that Facebook's practices were "not unique" and present "throughout the data analytics industry." The remaining Non-Flo Defendants employ similar data analytics practices.

## TOLLING, CONCEALMENT, ESTOPPEL, AND DELAYED DISCOVERY

241. The applicable statutes of limitation have been tolled as a result of Flo Health's knowing and active concealment and denial of the facts alleged herein, namely its practice of disclosing intimate health data to third parties without user consent.

242. Among other things, Flo Health made misrepresentations and omissions both publicly and in its Privacy Policy regarding its data sharing practices. Flo Health intentionally concealed the nature and extent of its actions and intentions. To the extent the Flo App made statements regarding Flo Health's service or its privacy policies, Flo Health either approved those statements or failed to timely correct them—in service of their ongoing scheme to conceal the true nature of their conduct.

243. Plaintiffs and Class members could not, with due diligence, have discovered the full scope of Flo Health's and the Non-Flo Defendants' conduct, due in no small part to Flo Health's deliberate efforts to conceal such conduct. All applicable statutes of limitation also have been tolled by operation of the discovery rule. Under the circumstances, Flo Health was under a duty to disclose the nature and significance of their data and privacy policies and practices but did not do so. Defendants are therefore estopped from relying on any statute of limitations.

244. Flo Health's and the Non-Flo Defendants' conduct is common to Plaintiffs and all Class members.

## CLASS ACTION ALLEGATIONS

245. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

> **Nationwide Class:** All natural persons in the United States who used the Flo App between June 2016 through present, inclusive (the "Class Period").[76]
>
> **California Subclass:** All natural persons residing in California who used the Flo App during the Class Period.

246. Excluded from the Classes are: (1) any Judge or Magistrate presiding over this action and any members of their immediate families; (2) the Defendants, Defendants' subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendants or their parents

[76] Plaintiffs have defined the Class based on currently available information and hereby reserves the right to amend the definition of the Class, including, without limitation, the Class Period.

have a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiffs' counsel and Defendants' counsel.

247. **Numerosity:** The exact number of members of the Class is unknown and unavailable to Plaintiffs at this time, but individual joinder in this case is impracticable. The Class likely consists of millions of individuals, and the members can be identified through Defendant Flo Health's records.

248. **Predominant Common Questions:** The Class' claims present common questions of law and fact, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant Flo Health violated Plaintiffs' and Class members' privacy rights;

b. Whether Defendant Flo Health's acts and practices violated California's Constitution, Art. 1, §1

c. Whether Defendant Flo Health's acts and practices amount to a breach of contract;

d. Whether Defendant Flo Health's acts and practices amount to a breach of implied contract;

e. Whether Defendants Flo Health, Facebook, Google, and Flurry were unjustly enriched;

f. Whether Defendant Flo Health violated the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*;

g. Whether Defendant Flo Health's acts and practices violated California's Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.*;

h. Whether Defendant Flo Health's acts and practices violated California's Business and Professions Code §17200, *et seq.*;

i. Whether the Defendants Facebook, Google, and Flurry's acts and practices violated California's Business and Professions Code §17200, *et seq.*;

j. Whether the Non-Flo Defendants aided and abetted Defendant Flo Health's violation of the California's Business and Professions Code §17200, *et seq.*;

k. Whether the Non-Flo Defendants aided and abetted Defendant Flo Health's tortious acts;

l. Whether Defendants Facebook, Google, and Flurry's acts and practices violated the Federal Wiretap Act, 18 U.S.C §§ 2510, *et seq.*;

m. Whether Defendants Facebook, Google, and Flurry's acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*

n. Whether Defendants Flo Health, Facebook, Google, and Flurry's acts and practices violated the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502;

o. Whether Plaintiffs and the Class members are entitled to equitable relief, including but not limited to, injunctive relief, restitution, and disgorgement; and,

p. Whether Plaintiffs and the Class members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

249. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of the Class. The claims of Plaintiffs and the members of the Class arise from the same conduct by Defendants and are based on the same legal theories.

250. **Adequate Representation:** Plaintiffs have and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiffs have retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiffs have no interest that is antagonistic to the interests of the Class, and Defendants have no defenses unique to any Plaintiffs. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to the interests of the other members of the Class.

251. **Substantial Benefits:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

252. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

**CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS**

253. California substantive laws apply to each member of the Class. Flo Health's Terms of Use states "These Terms of Use (this 'Agreement') is a legal agreement between [users] and Flo Health, Inc."

254. This agreement states that "[a]ny dispute arising from this Agreement shall be governed by the laws of the State of California without regard to its conflict of law provisions. Sole and exclusive jurisdiction for any action or proceeding arising out of or related to this agreement shall be in an appropriate state or federal court located in San Francisco County, State of California . . . ."[77]

255. By choosing California law for the resolution of disputes in the agreement, Flo Health concedes that it is appropriate for this Court to apply California law to the instant dispute.

256. Further, California's substantive laws may be constitutionally applied to the claims of Plaintiffs and the Class under the Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the U.S. Constitution. California has significant contact, or significant aggregation of contacts, to the claims asserted by Plaintiffs and Class members, thereby creating state interests to ensure that the choice of California state law is not arbitrary or unfair.

257. Flo Health maintains a California executive office at 541 Jefferson Ave, Suite 100, Redwood City, CA 94063-1700, where Defendant Flo Health's Chief Executive Officer and Chief Financial Officer, Maxim Scrobov and Secretary Constantin Luchian work from.[78] Defendant Flo Health also conducts substantial business in California, such that California has an interest in regulating Defendant Flo Health's conduct under its laws. Defendant Flo Health's decision to reside

[77] *Terms of Use*, FLO HEALTH, INC. (effective Feb. 5, 2020), https://flo.health/terms-of-service.

[78] *Flo Health, Inc. Statement of Information*, SEC'Y OF STATE OF THE STATE OF CAL. (Sept. 27, 2019), https://businesssearch.sos.ca.gov/Document/RetrievePDF?Id=04312974-26956704.

in California and avail itself of California's laws, renders the application of California law to the claims herein constitutionally permissible.

258. The application of California laws to the Class is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiffs and the proposed Class, and California has a greater interest in applying its laws here than any other interested state.

## CLAIMS FOR RELIEF

### FIRST CLAIM FOR RELIEF
**Violation Common Law Invasion of Privacy – Intrusion Upon Seclusion**
**Against Flo Health**
**(On Behalf of Plaintiffs and the Class and Subclass)**

259. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

260. Plaintiffs' asserting claims for intrusion upon seclusion must plead (1) that the Defendant Flo Health intentionally intruded into a place, conversation, or matter as to which Plaintiffs had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

261. Flo Health's disclosure of Plaintiffs' and Class members' intimate health data, including information concerning physical and emotional health, family planning, and romantic lifestyle, as well as their interests in making intimate personal decisions or conducting personal activities, constitutes an intentional intrusion upon Plaintiffs' and Class members' solitude or seclusion in that Flo Health shared these intimate personal details that were intended to stay private with third parties without users' consent, and despite Flo Health's express promises that it would not do so.

262. Plaintiffs and Class members had a reasonable expectation of privacy in their intimate health data. Plaintiffs and Class members did not consent to, authorize, or know about Flo Health's intrusion at the time it occurred. Plaintiffs and Class members never agreed that Flo Health could disclose their intimate health data.

263. Plaintiffs and Class members did not consent to, authorize, or know about Flo Health's intrusion at the time it occurred. Plaintiffs and Class members never agreed that their intimate health data would be collected or disclosed to third parties, including to the Non-Flo Defendants.

264. Flo Health's intentional intrusion on Plaintiffs' and Class members' solitude or seclusion without consent would be highly offensive to a reasonable person. Plaintiffs and Class members reasonably expected, based on Flo Health's repeated assurances, that their intimate health data would not be disclosed. Flo Health's conduct is especially egregious as it failed to contractually restrict what third parties do with Plaintiffs' and Class members' intimate health data once it is disclosed.

265. The surreptitious taking and disclosure of intimate health data from thousands if not millions of individuals was highly offensive because it violated expectations of privacy that have been established by social norms. Privacy polls and studies show that the overwhelming majority of Americans believe one of the most important privacy rights is the need for an individual's affirmative consent before personal data is collected or shared. Moreover, the disclosure and collection of intimate health data by Flo Health violated its own privacy disclosures and representations.

266. Given the extremely intimate nature of the data Flo Health collected and disclosed, such as private details about users' sexual activity, menstrual cycles, and physical and mental health, this kind of intrusion would be (and in fact is) highly offensive to a reasonable person.

267. The highly offensive nature of Flo Health's intentional intrusion into Plaintiffs' and Class members' personal affairs is confirmed by its FTC settlement and the public outrage and hundreds of complaints received by Flo Health after its data sharing practices were disclosed, instructing Flo Health to delete their data or their accounts or that they would be deleting their accounts.

268. Users have expressed extreme outrage in response to Flo Health's data sharing practices:

a. "I'm absolutely [sic] disgusted at this invasion of my most personal information."

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 party?"[79]

269. Alice Berg, a 25-year old student, told the *Wall Street Journal*, "I think it's incredibly dishonest of them that they're just lying to their users especially when it comes to something so sensitive."[80]

270. As a result of Flo Health's actions, Plaintiffs and Class members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

271. Plaintiffs and Class members have been damaged as a direct and proximate result of Flo Health's invasion of their privacy and are entitled to just compensation, including monetary damages.

272. Plaintiffs and Class members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs and Class members for the harm to their privacy interests as well as a disgorgement of profits made by Flo Health as a result of its intrusions upon Plaintiffs' and Class members' privacy.

273. Plaintiffs and Class members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Flo Health's actions, directed at injuring Plaintiffs and Class members in conscious disregard of their rights. Such damages are needed to deter Flo Health from engaging in such conduct in the future.

274. Plaintiffs also seek such other relief as the Court may deem just and proper.

---

[79] Complaint, *In the Matter of Flo Health Inc.*, FEDERAL TRADE COMMISSION, No. 1923133, https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf.

[80] Sam Schechner and Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL STREET JOURNAL, (Feb. 22, 2019 11:07 AM), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

**SECOND CLAIM FOR RELIEF**
**Invasion of Privacy and Violation of the California Constitution, Art. 1, § 1**
**Against Flo Health**
**(On Behalf of Plaintiffs and the Class and Subclass)**

275. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

276. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." California Constitution, Article I., Section 1.

277. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

278. The right to privacy in California's constitution creates a right of action against private and government entities.

279. Plaintiffs and Class members have and continue to have a reasonable expectation of privacy in their personal information, identities, data, and medical information pursuant to Article One, Section One of the California Constitution.

280. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances, including that: (i) the data collected by Defendant Flo Health included personal, intimate, decisions, including whether to bear children, their menstruation cycles, and fertility issues; (ii) Plaintiffs and Class members did not consent or otherwise authorize Flo Health to collect and disclose this private information with the Non-Flo Defendants for their own monetary gain; and (iii) Flo Health affirmatively assured Plaintiffs and Class members that this information would not be disclosed unless as needed to provide Flo Health's services.

281. The confidential and sensitive information, which Flo Health intruded upon, intercepted, collected, and disclosed without Plaintiffs' and Class members' authorization or consent, included intimate health data, such as information concerning physical and emotional

health, family planning, and romantic lifestyle, as well as Plaintiffs' interests in making intimate personal decisions or conducting personal activities.

282. Flo Health's actions constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that: (i) the data collected was highly sensitive and personal, as protected by the California Constitution; (ii) Defendants did not have authorization or consent to collect this information; and (iii) the invasion deprived Plaintiffs and Class members the ability to control the circulation of said information, which is considered a fundamental right to privacy.

283. Flo Health's invasion violated the privacy rights of hundreds of thousands of Class members, including Plaintiffs, without authorization or consent. Flo Health's conduct constitutes a severe and egregious breach of social norms.

284. As a result of Flo Health's actions, Plaintiffs and Class members have sustained damages and will continue to suffer damages as a direct and proximate result of Flo Health's invasion of privacy.

285. Plaintiffs and Class members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs and Class members for the harm to their privacy interests as well as a disgorgement of profits made by Flo Health as a result of its intrusions upon Plaintiffs' and Class members' privacy.

286. Plaintiffs and Class members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Flo Health's actions, directed at injuring Plaintiffs and Class members in conscious disregard of their rights. Such damages are needed to deter Flo Health from engaging in such conduct in the future.

287. Plaintiffs also seeks such other relief as the Court may deem just and proper.

**THIRD CLAIM FOR RELIEF**
**Breach of Contract against Flo Health**
**(On Behalf of Plaintiffs and the Class and Subclass)**

288. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

289. Plaintiffs entered into a contract with Flo Health by downloading and using the Flo App. In connection with using the Flo App, both parties agree to abide by Flo Health's Terms of Use ("TOU"). Plaintiffs have fully complied with their obligations under the TOU with regard to their use of Flo Health's product and services.

290. The TOU states that "[b]y creating an account or accessing or using the App, you acknowledge that you accept and agree to be bound by the terms of this Agreement." Plaintiffs and Defendant Flo Health are subject to Flo Health's Privacy Policy, which is incorporated into the TOU.[81]

291. Defendant Flo Health's Privacy Policy states that it only provides users' personal data to third parties when that data "is reasonably necessary to perform their work," which may include "suppl[ying] software applications, web hosting, and other technologies for the App." Flo Health breached the contract because it did not disclose this information to "provide services in connection with the App."[82] Flo Health allowed third parties to use this information for any purpose, including for the third party's own benefit, research, development, and targeted advertising that was unrelated to the stated purpose disclosed by the Privacy Policy.

292. Flo Health's Privacy Policy stated that any information shared with third parties "exclud[ed] information regarding your marked cycles, pregnancy, symptoms, notes and other information that is entered by you and that you do not elect to share."[83] Flo Health breached the contract because it disclosed users' intimate health data regarding marked cycles, fertility cycles, pregnancy and other health information in the form of Custom App Events to third parties.

293. Flo Health's Privacy Policy stated that Flo Health would not disclose "any data related to health" to either of the mobile analytics firms AppsFlyer or Flurry. Flo Health breached

---

[81] *Terms of Use*, FLO HEALTH, INC. (effective Feb. 5, 2020), https://flo.health/terms-of-service.

[82] *Privacy Policy*, FLO HEALTH, INC. (effective July. 16, 2018) , https://flo.health/privacy-policy-archived/july-16-2018.

[83] *Id.*

the contract because it disclosed to AppsFlyer and Flurry Custom App Events which contained intimate health data.

294. Flo Health's Privacy Policy stated that Flo Health would only provide "non-personally identifiable information," "Personal Data like device identifiers," or "device identifiers"[84] to Facebook, Google, and Fabric. Flo Health breached the contract because it provided Facebook, Google, and Fabric access to Custom App Events which conveyed identifiable information and intimate health data, unlike device identifiers.

295. By disclosing Plaintiffs' and Class members' intimate health data to third parties, including the Non-Flo Defendants, without their consent, Defendant Flo Health has breached material terms of the contract.

296. Had Plaintiffs and Class members known that Flo Health would disclose their intimate health data to third parties without their consent, they would not have contracted with Flo Health.

297. As a result of Flo Health's breach of contract, Plaintiffs and Class members have suffered damages in an amount to be determined at trial. In addition, or in the alternative, Plaintiffs and Class members seek damages that will reasonably compensate Plaintiffs and Class members for the harm to their privacy interest. By sharing their intimate health data with third parties without consent, Flo Health invaded Plaintiffs' and Class members' privacy interests. As a result of Flo Health's breach of the TOU and Privacy Policy, Plaintiffs and Class members have suffered damages.

**FOURTH CLAIM FOR RELIEF**
**Breach of Implied Contract Against Flo Health**
**(On Behalf of Plaintiffs and the Class and the Subclass)**
**(In the Alternative)**

298. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

299. Plaintiffs allege this claim in the alternative to their Third Claim for Relief.

[84] *Id.*

300. Plaintiffs entered into an implied contract with Defendant Flo Health by downloading and using the Flo App. In connection with using the Flo App, both parties agree to abide by Flo Health's Terms of Use ("TOU"). Plaintiffs have fully complied with their obligations under the TOU with regard to their use of Flo Health's product and services.

301. Defendant Flo Health solicited and invited prospective customers such as Plaintiffs and Class members to use the Flo App with claims that Flo Health cares about Plaintiffs' and Class members' privacy rights.

302. Flo Health's offer included specific assurances from Flo Health's Privacy Policy, including that Flo Health would only share "certain" personal data with third parties, limited to only the "information that is reasonably necessary to perform their work" in support of the Flo App.[85]

303. Plaintiffs and Class members accepted Flo Health's offers by downloading the Flo App and entering intimate health data into the Flo App because of these promises.

304. In entering into such implied contracts, Plaintiffs and Class members reasonably believed that Flo Health would comply with relevant laws and regulations, including privacy laws, as well as the Flo Health's own assurances.

305. Plaintiffs and Class members reasonably believed that Flo Health would not disclose intimate information regarding their fertility cycles, lifestyle choices, and romantic relationships with third parties, as stated in its Privacy Policy.

306. Flo Health's implied promise not to disclose Plaintiffs' and Class members' sensitive personal information to third parties is evidenced by, e.g., the representations in Flo Health's terms of use and Privacy Policy set forth above.

307. Plaintiffs and Class members would not have downloaded or made use of the Flo App in the absence of such promises.

[85] *Id.*

308. Plaintiffs and Class members fully performed their obligations under the implied contracts with Flo Health by abstaining from making any "forbidden use" of the Flo App, as dictated by the Flo Health's terms of service.[86]

309. Flo Health breached its implied contract with Plaintiffs and Class members by secretly collecting and disclosing sensitive personal data for Flo Health's own benefit, in violation of the terms of use and Privacy Policy.

310. By disclosing Plaintiffs' and Class members' intimate health data to third parties without their consent, Flo Health has breached material terms of the implied contract.

311. As a result of Flo Health's breach of implied contract, Plaintiffs and Class members have suffered damages in an amount to be determined at trial. In addition, or in the alternative, Plaintiffs and Class members seek damages that will reasonably compensate Plaintiffs and Class members for the harm to their privacy interest. By sharing their intimate health data with third parties without consent, Flo Health invaded Plaintiffs' and Class members' privacy interests. As a result of Flo Health's breach of the TOU and Privacy Policy, Plaintiffs and Class members have suffered damages.

**FIFTH CLAIM FOR RELIEF**
**Unjust Enrichment Against Flo Health, Facebook, Google, and Flurry**
**(On Behalf of Plaintiffs and the Class and Subclass)**
**(In the Alternative as to Flo Health)**

312. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

313. As to Flo Health, Plaintiffs allege this claim in the alternative to their Third Claim for Relief.

314. Defendants received benefits from Plaintiffs and Class members and unjustly retained those benefits at their expense.

315. Plaintiffs and Class members conferred a benefit upon Flo Health in the form of valuable sensitive personal data that Flo Health collected from Plaintiffs and Class members,

[86] *Terms of Use*, FLO HEALTH, INC. (effective Feb. 5, 2020), https://flo.health/terms-of-service.

without authorization and proper compensation. Flo Health has collected, disclosed, and otherwise misused this information for its own gain, providing Flo Health with economic, intangible, and other benefits, including substantial monetary compensation from third parties who received Plaintiffs' and Class members' sensitive personal data.

316. Plaintiffs and Class members conferred a benefit upon Facebook, Google, and Flurry in the form of valuable sensitive personal data that Facebook, Google, and Flurry received and used, without authorization and proper compensation. Facebook, Google, and Flurry received, analyzed, and otherwise misused this information for their own gain, providing those Defendants with economic, intangible, and other benefits, including profits from their data and analytics business and marketing activities.

317. Defendants unjustly retained those benefits at the expense of Plaintiffs and Class members because Defendants' conduct damaged Plaintiffs and Class members, all without providing any commensurate compensation to Plaintiffs and Class members.

318. The benefits that Defendants derived from Plaintiffs and Class members rightly belong to Plaintiffs and Class members. It would be inequitable under unjust enrichment principles in California and every other state for Defendants to be permitted to retain any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

319. Defendants should be compelled to disgorge in a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds that Defendants received, and such other relief as the Court may deem just and proper.

## SIXTH CLAIM FOR RELIEF
**Stored Communications Act ("SCA") Against Flo Health**
**18 U.S.C. §§ 2702, *et seq.***
**(On Behalf of Plaintiffs and the Class and Subclass)**

320. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

321. The SCA provides that a person "providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service[.]" 18 U.S.C. § 2702(a)(1).

322. "Electronic communication" is broadly defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce[.]" 18 U.S.C. § 2510(12).

323. "Electronic storage" is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and . . . any storage of such communication by an electronic communication service for purposes of backup protection of such communication[.]" 18 U.S.C. § 2510(17)(A)-(B).

324. "Electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications[.]" 18 U.S.C. § 2510(15).

325. "Person" is defined as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

326. Flo Health, as a corporation, is a person as defined under 18 U.S.C. § 2510(6).

327. The Non-Flo Defendants are persons as defined under 18 U.S.C. § 2510(6).

328. Plaintiffs and Class members, as individuals, are persons as defined under 18 U.S.C. §2510(6).

329. Plaintiffs and Class members reasonably expected that Flo Health's service did not include disclosing their "electronic communications," i.e., their data (as broadly defined). Plaintiffs' and Class members' expectation was based, in part, on Flo Health's failure to provide ***any*** disclosures or obtain consent for permission to do so, as well as Flo Health's affirmative misrepresentations that it would not disclose this information. The Non-Flo Defendants were not an intended party or recipient of Plaintiffs' and Class members' intimate health data. Plaintiffs and

Class Members did not consent or authorize Flo Health to disclose their communications to any third parties, including the Non-Flo Defendants.

330. Flo Health stores Plaintiffs' and Class members' electronic communications for back-up purposes in the event that a user needs to restore their account. During this period, Flo Health, without authorization, intentionally divulged and transmitted Plaintiffs' and Class members' personal health data to third parties, including the Non-Flo Defendants.

331. Flo Health knowingly divulged the contents of Plaintiffs' and Class members' communications while they were in electronic storage to third parties, including the Non-Flo Defendants, in intentional or in reckless disregard for Plaintiffs' and Class members' privacy rights. Flo Health did so for its own benefit, and for the benefit of the Non-Flo Defendants, including in order to increase and improve their marketing and advertising efforts.

332. Flo Health's actions were at all relevant times knowing, willful, and intentional, as evidenced by the fact that this was Flo Health's routine business practice and it purposefully failed to disclose this practice to consumers.

333. As a result of Flo Health's violations of the SCA, Plaintiffs and Class members have suffered harm and injury, including but not limited to the invasion of their privacy rights.

334. Pursuant to 18 U.S.C. § 2707, Plaintiffs and Class members are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the sum of the actual damages suffered by Plaintiffs and the Class and any profits made by Flo Health as a result of the violation, but in no case less than the minimum statutory damages of $1,000 per person; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

**SEVENTH CLAIM FOR RELIEF**
**Violation of California Confidentiality of Medical Information Act**
**Against Flo Health**
**Civil Code Section 56 *et seq.***
**("CMIA")**
**(On Behalf of Plaintiffs and the Class and Subclass)**

335. Plaintiffs re-allege and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

336. Flo Health is deemed a provider of health care under Cal. Civ. Code Section 56.06, subdivision (b), because it offers software to consumers that is designed to maintain medical information for the purposes of allowing its users to manage their information or for the diagnosis, treatment, or management of a medical condition.

337. Plaintiffs and Class members are "Patients" as defined by Cal. Civ. Code Section 56.05(k).

338. The Flo App is designed for users to store personally identifiable information relating to their reproductive health, such as ovulation and menstrual cycles, and/or for the diagnoses, treatment, or management of users seeking to become pregnant or treat infertility. This information is "Medical Information" as defined by Cal. Civ. Code Section 56.05(j).

339. Flo Health is therefore subject to the requirements of the CMIA and obligated under subdivision (d) to maintain the same standards of confidentiality required of a provider of health care with respect to Medical Information that it maintains on behalf of users.

340. Flo Heath stored in electronic form on its systems Plaintiffs' and Class members' Medical Information as defined in Cal. Civ. Code Section 56.05(j).

341. Plaintiffs and Class members did not provide Flo Health authorization, nor was Flo Health otherwise authorized to disclose Plaintiffs' and Class members' Medical Information to an authorized third party, such as the Non-Flo Defendants.

342. In violation of the CMIA, Flo Health knowingly and willfully disclosed the Medical Information of Plaintiffs and Class members without first obtaining "authorization," for its own financial gain.

343. Specifically, Flo Health violated Cal. Civil Code Section 56.10, subdivision (a) which prohibits a health care provider from disclosing medical information without first obtaining an "authorization," unless a statutory exception applies. Flo Health did not follow any of the proper procedures enumerated in Cal. Civil Code Section 56.11 to obtain proper authorization.

344. Flo Health disclosed medical information without first obtaining authorization when it disclosed to third parties, including the Non-Flo Defendants, Plaintiffs' and Class members' intimate health data without consent, including information concerning physical and emotional health, family planning, and romantic lifestyle, as well as their interests in making intimate personal decisions or conducting personal activities. No statutory exception applies.

345. This information was shared with third parties, including the Non-Flo Defendants, whose business is to sell advertisements based on that data it collects about individuals, including the data Plaintiffs and the Class shared with the Flo App.

346. This release of Plaintiffs' and Class members' Medical Information to third parties, including the Non-Flo Defendants, was an affirmative act in violation of Cal. Civ. Code Section 56.10(a).

347. Cal. Civ. Code Section 56.10(d) reinforces these restrictions by stating that unless "expressly authorized by a patient, enrollee, or subscriber, or as provided by subdivisions (b) or (c), a provider of health care . . . shall not intentionally share, sell, use for marketing, or otherwise use medical information for a purpose not necessary to provide health care services to the patient."

348. As a direct and proximate result of Flo Health's violation of Cal. Civ. Code Section 56.10(a), Plaintiffs' and Class members' Medical Information was viewed.

349. Flo Health's unauthorized disclosures of Plaintiffs' and Class members' Medical Information has caused injury to Plaintiffs and Class members.

350. In addition, Cal. Civil Code Section 56.101, subdivision (a), requires that every provider of health care "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein."

351. Flo Health failed to maintain, preserve, and store medical information in a manner that preserves the confidentiality of the information contained therein because it disclosed to third parties Plaintiffs' and Class members' intimate health data without consent, including information concerning physical and emotional health, family planning, and romantic lifestyle, as well as their interests in making intimate personal decisions or conducting personal activities.

352. Thus, Flo Health shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Cal. Civ. Code Section 56.36.

353. Accordingly, Plaintiffs and Class members are entitled to: (1) nominal damages of $1,000 per violation; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant to 56.36(c); (4) punitive damages pursuant to Cal. Civ. Code Section 56.35; and (5) reasonable attorneys' fees and other litigation costs reasonably incurred.

**EIGHTH CLAIM FOR RELIEF**
**Violations of Cal. Bus. & Prof. Code §§ 17200 *et. seq.* Against Flo Health**
**(On Behalf of Plaintiffs and the Class and Subclass)**

354. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

355. Flo Health's business acts and practices are "unlawful" under the Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et. seq*. ("UCL"), because, as alleged above, Flo Health violated the California common law, California Constitution, and the other State and Federal statutes and causes of action described herein.

356. Flo Health's business acts and practices are "unfair" under the UCL. California has a strong public policy of protecting consumers' privacy interests, including protecting consumers' personal data. Flo Health violated this public policy by, among other things, surreptitiously collecting, disclosing, and otherwise misusing Plaintiffs' and Class members' sensitive personal data without Plaintiffs' and Class members' consent. Flo Health further engaged in unfair business practices because it made material misrepresentations and omissions concerning the information

that Flo Health assured users it would not share with third parties, which deceived and misled users of the Flo App. Flo Health's conduct violates the policies of the statutes referenced herein.

357. Flo Health's business acts and practices are also "unfair" in that they are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers. The gravity of the harm of Flo Health secretly collecting, disclosing, and otherwise misusing Plaintiffs' and Class members' sensitive personal data is significant, and there is no corresponding benefit resulting from such conduct. Finally, because Plaintiffs and Class members were completely unaware of Flo Health's conduct, they could not have possibly avoided the harm.

358. Flo Health's business acts and practices are also "fraudulent" within the meaning of the UCL. Flo Health has amassed a large collection of sensitive personal data without disclosing this practice and therefore acted without consumers' knowledge or consent. Flo Health's business acts and practices were likely to, and did, deceive members of the public including Plaintiffs and Class members into believing this data was private. Flo Health assured users that only ***certain data*** (like technical identifiers) would be disclosed as necessary, such as "to provide services in connection with the App." Flo Health deceived users into believing that under no circumstances would the Flo Health disclose "information regarding [users'] marked cycles, pregnancy, symptoms, notes and other information entered by [users]" or "survey results." Flo Health did not disclose that it would share this data with third parties, including the Non-Flo Defendants. Such information was not kept private, as Flo Health secretly collected, disclosed, and otherwise misused this data by sharing it with the Non-Flo Defendants for their own purposes.

359. Flo Health's violations were, and are, willful, deceptive, unfair, and unconscionable.

360. Had Plaintiffs and Class members known that their information would be collected, and otherwise misused for Flo Health's own benefit, they would not have used the Flo App.

361. Plaintiffs and Class members have a property interest in their sensitive personal data. By surreptitiously collecting and otherwise misusing Plaintiffs' and Class members' information, Defendants have taken property from Plaintiffs and Class members without providing just or any compensation.

362. Plaintiffs and Class members have lost money and property as a result of Flo Health's conduct in violation of the UCL, as stated in herein and in Section E, *supra*. Health data, such as the data collected by Flo Health, objectively has value. Companies are willing to pay for health data, like the data collected and shared with the Non-Flo Defendants by Flo Health. For instance, Pfizer annually pays approximately $12 million to purchase health data from various sources.[87]

363. Consumers also value their health data. According to the annual Financial Trust Index Survey, conducted by the University of Chicago's Booth School of Business and Northwestern University's Kellogg School of Management, which interviewed more than 1,000 Americans, 93 percent would not share their health data with a digital platform for free. Half of the survey respondents would only share their data for $100,000 or more, and 22 percent would only share their data if they received between $1,000 and $100,000.[88]

364. By deceptively taking and sharing this data with the Non-Flo Defendants, Flo Health has taken money or property from Plaintiffs and Class members.

365. For these reasons, Plaintiffs seek restitution and compensatory damages on behalf of themselves and Class members.

**NINTH CLAIM FOR RELIEF**
**Violations of Cal. Bus. & Prof. Code §§ 17200 *et. seq.* Against Facebook, Google, and Flurry**
**(On Behalf of Plaintiffs and the Class and Subclass)**

366. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

---

[87] Adam Tanner, *How Data Brokers Make Money Off Your Medical Records*, SCI. AM. (Feb. 1, 2016), https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/.

[88] Andrea Park, *How much should health data cost? $100K or more, according to patients*, BECKER'S HOSP. REV. (Feb. 12, 2020), https://www.beckershospitalreview.com/healthcare-information-technology/how-much-should-health-data-cost-100k-or-more-according-to-patients.html.

367. Facebook, Google, and Flurry's business acts and practices are "unlawful" under the UCL, because those Defendants violated the California common law and the other statutes and causes of action described herein.

368. Facebook, Google, and Flurry's business acts and practices are "unfair" under the UCL. California has a strong public policy of protecting consumers' privacy interests, including protecting consumers' personal data. Those Defendants violated this public policy by, among other things, secretly receiving and using Plaintiffs' and Class members' sensitive personal data without Plaintiffs' and Class members' knowledge or consent. The Defendants' conduct violates the policies of the statutes referenced herein.

369. Facebook, Google, and Flurry's business acts and practices are also "unfair" in that they are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers. The gravity of the harm of Facebook, Google, and Flurry's conduct in secretly receiving and using Plaintiffs' and Class members' sensitive personal data is significant and there is no corresponding benefit resulting from such conduct. Finally, because Plaintiffs and Class members were completely unaware of Facebook, Google, and Flurry's conduct, they could not have possibly avoided the harm.

370. Facebook, Google, and Flurry's business acts and practices are also "fraudulent" within the meaning of the UCL. Those Defendants have amassed a large collection of sensitive personal data without disclosing this practice and therefore without consumers' knowledge or consent. Facebook, Google, and Flurry designed their SDKs to blend seamlessly with apps like Flo Health, so that users are unaware that Defendants collect their sensitive personal data. Through these practices, Plaintiffs and Class members were deceived into believing they were only sharing data with Flo Health and not third parties, such as Facebook, Google, and Flurry.

371. Had Plaintiffs and Class members known that their information would be sent to and used by Facebook, Google, and Flurry for their own benefit, they would not have used the Flo Health app, which incorporates Defendants' SDKs.

372. Plaintiffs and Class members have a property interest in their sensitive personal data. By surreptitiously collecting and otherwise misusing Plaintiffs' and Class members' information,

Defendants have taken property from Plaintiffs and Class members without providing just or any compensation.

373. Plaintiffs and Class members have lost money and property as a result of the Defendants' conduct in violation of the UCL, as stated herein and in section E, *supra*.

374. Consumers also value their health data. According to the annual Financial Trust Index Survey, conducted by the University of Chicago's Booth School of Business and Northwestern University's Kellogg School of Management, which interviewed more than 1,000 Americans, 93 percent would not share their health data with a digital platform for free. Half of the survey respondents would only share their data for $100,000 or more, and 22 percent would only share their data if they received between $1,000 and $100,000.

375. By deceptively receiving and using Plaintiffs' and Class members' sensitive data, Facebook, Google, and Flurry have taken money or property from Plaintiffs and Class members.

376. For these reasons, Plaintiffs seek restitution and compensatory damages on behalf of themselves and Class members.

**TENTH CLAIM FOR RELIEF**
**Aiding and Abetting Violations of**
**Cal. Bus. & Prof. Code §§ 17200 *et. seq.* Against the Non-Flo Defendants**
**(On Behalf of Plaintiffs and the Class and Subclass)**

377. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

378. As set forth herein, Flo Health's disclosure of Plaintiffs' and Class members' intimate health data was "unfair," "unlawful," and "fraudulent" within the meaning of the Cal. Bus. & Prof. Code §§ 17200 *et. seq.* such that Plaintiffs and Class members have lost money and property as a result of Flo Health's conduct in violation of the UCL.

379. By contracting with Flo Health to receive Plaintiffs' and Class members' intimate health data for their own financial gain, and by virtue of their access to Flo Health's Privacy Policy, the Non-Flo Defendants acted with knowledge that Flo Health's misrepresentations and/or omissions regarding the use of such data would be (a) unlawful under current state or federal law;

(b) "unfair," in that Flo Health's business practice was immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers, and/or (c) fraudulent in that members of the public were likely to be deceived by Flo Health's misrepresentations and/or omissions.

380. The Non-Flo Defendants provided substantial assistance and encouragement to Flo Health's unlawful, unfair, and fraudulent business practices by entering into agreements with Flo Health to receive, collect, and analyze Plaintiffs' and Class members' intimate health data.

381. The Non-Flo Defendants used their access to Flo Health to collect data about Flo Health users that they would not otherwise have received through their SDKs. The Non-Flo Defendants supplied Flo Health with the SDKs to collect, analyze, and share users' intimate health data. The Non-Flo Defendants knew that their SDKs could be seamlessly integrated without alerting users that their intimate health data would be shared with third parties.

382. The Non-Flo Defendants' agreements with Flo Health and receipt of Plaintiffs' and the Class members' intimate health data were substantial factors in causing the unfair, unlawful, and fraudulent business practices to the Plaintiffs and the Class alleged herein. The Non-Flo Defendants used this personal and intimate health information to develop, profile, and target users, such as Plaintiffs, for advertisements and the Non-Flo Defendants' own purposes, including advertisement, marketing campaigns, research and product development.

383. As a result, the Non-Flo Defendants aided and abetted Flo Health's violation of Cal. Bus. & Prof. Code §§ 17200 *et. seq.* and are therefore jointly liable with Flo Health for the relief sought by Plaintiffs and the Class. Plaintiffs and Class members have lost money and property as a result of the Non-Flo Defendants' conduct, as stated in herein and in Section E, *supra*.

**ELEVENTH CLAIM FOR RELIEF**
**Aiding and Abetting Violation Common Law Invasion of Privacy – Intrusion Upon Seclusion Against the Non-Flo Defendants**
**(On Behalf of Plaintiffs and the Class and Subclass)**

384. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

385. As set forth herein, Flo Health's disclosure of Plaintiffs' and Class members' intimate health data, including information concerning physical and emotional health, family planning, and romantic lifestyle, as well as their interests in making intimate personal decisions or conducting personal activities, constitutes an intentional intrusion upon Plaintiffs' and Class members' solitude or seclusion. Flo Health shared these intimate personal details that were intended to stay private with third parties, including the Non-Flo Defendants, without users' consent, and despite Flo Health's express promises that it would not do so.

386. By contracting with Flo Health to receive Plaintiffs' and Class members' intimate health data for their own financial gain, and by virtue of their access to Flo Health's Privacy Policy, the Non-Flo Defendants acted with knowledge that Flo Health's misappropriation of Plaintiffs' and the Class members' intimate personal information was an intentional intrusion upon Plaintiffs' and Class members' solitude or seclusion.

387. The Non-Flo Defendants provided substantial assistance and encouragement to Flo Health's invasion of Plaintiffs' and the Class' privacy by entering into agreements with Flo Health to receive, collect, and analyze Plaintiffs' and the Class' intimate health data.

388. The Non-Flo Defendants used their access to Flo Health to collect data about Flo Health users that they would not otherwise have received through their SDKs. The Non-Flo Defendants supplied Flo Health with the SDKs to collect, analyze, and share users' intimate health data. The Non-Flo Defendants knew that their SDKs could be seamlessly integrated without alerting users that their intimate health data would be shared with third parties.

389. The Non-Flo Defendants' agreements with Flo Health and receipt of Plaintiffs' and the Class members' intimate health data was a substantial factor in causing the privacy harms to Plaintiffs and the Class alleged herein.

390. For example, the Non-Flo Defendants used this information to develop profiles and target users, such as Plaintiffs, for advertisements and marketing campaigns. Given the lucrative nature of users' health data, the Non-Flo Defendants were willing to receive, and encouraged, Flo Health to share users' intimate health data.

391. As a result, the Non-Flo Defendants aided and abetted Flo Health's tortious invasion of the Plaintiffs' and the Class members' privacy and are therefore jointly liable with Flo Health for the relief sought by Plaintiffs and the Class.

**TWELTH CLAIM FOR RELIEF**
**Violation of the Federal Wiretap Act Against Facebook, Google, and Flurry**
**18 U.S.C §§ 2510, *et seq.***
**(On Behalf of Plaintiffs and the Class and Subclass)**

392. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

393. The Federal Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*, prohibits the interception of, or the endeavors to intercept, any wire, oral, or electronic communications without the consent of at least one authorized party to the communication. The statute confers a civil cause of action on "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

394. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

395. "Contents" is defined as "includ[ing] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

396. "Person" is defined as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

397. "Electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . ." 18 U.S.C. § 2510(12).

398. Flo Health, Facebook, Google, and Flurry are persons for purposes of the Wiretap Act because they are corporations.

399. The Flo App is a device for purposes of the Wiretap Act because it is software used to intercept oral and electronic communication.

400. Plaintiffs' and Class members' intimate health data which was intercepted by Defendants are "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

401. Plaintiffs and Class members reasonably expected that Facebook, Google, and Flurry were not intercepting, recording, or disclosing their electronic communications, based on Flo Health's misrepresentations.

402. Plaintiffs and Class members' electronic communications were intercepted during transmission, without their consent and for the unlawful and/or wrongful purpose of monetizing their private information, including by using their private information to develop marketing and advertisement strategies, without Plaintiffs' and Class members' consent.

403. Interception of Plaintiffs' and Class members' private and confidential electronic communications without their consent occurs whenever users engage with the Flo App. Facebook, Google, and Flurry are not parties to these communications.

404. Defendants' actions were at all relevant times knowing, willful, and intentional, particularly because Facebook, Google, and Flurry are sophisticated parties who know the type of data they intercept through their own products, i.e., SDKs.

405. Neither Plaintiffs nor the Class consented to Facebook, Google, and Flurry's interception, disclosure, and/or use of their intimate health data in their electronic communications with the Flo App. Nor could they—Facebook, Google, and Flurry (as well as Flo Health) never sought to, or did, obtain Plaintiffs' or the Class members' consent.

406. Pursuant to 18 U.S.C. § 2520, Plaintiffs and Class Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the Wiretap Act and are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Class and any profits made by Defendants as a result of the violation, or (b) statutory

damages of whichever is the greater of $100 per day per violation or $10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

**THIRTEENTH CLAIM FOR RELIEF**
**Violation of the California Invasion of Privacy Act Against Facebook, Google, and Flurry**
**Cal. Penal Code §§ 630, *et seq*. ("CIPA")**
**(On Behalf of Plaintiffs and the Class and Subclass)**

407. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

408. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.* ("CIPA") finding that "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630. Thus, the intent behind CIPA is "to protect the right of privacy of the people of this state." *Id.*

409. Cal. Penal Code § 632 prohibits eavesdropping upon or recording of any confidential communication, including those occurring among the parties in the presence of one another or by means of a telephone, telegraph, or other device, through the use of an electronic amplifying or recording device without the consent of all parties to the communication.

410. By contemporaneously intercepting and accessing Plaintiffs' and Class members' intimate health data communicated to the Flo App via SDKs, Facebook, Google, and Flurry, without consent and authorization of all parties, eavesdropped and/or recorded confidential communications through an electronic amplifying or recording device in violation of § 631(a) of the CIPA.

411. Facebook, Google, and Flurry, through the transfer of data via SDKs, utilized Flo App user's personal health information for their own purposes. Indeed, from June 2016 to February

2019, Facebook utilized Flo App users' personal health information for its own research and product development.[89]

412. Plaintiffs and the Class members seek statutory damages in accordance with § 637.2(a), which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiffs and the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

413. Plaintiffs and Class members have also suffered irreparable injury from these unauthorized acts of disclosure, their personal, private, and sensitive health information have been collected, viewed, accessed, stored, and used by Defendants, and have not been destroyed, and due to the continuing threat of such injury, have no adequate remedy at law, Plaintiffs and Class members are entitled to injunctive relief.

**FOURTEENTH CLAIM FOR RELIEF**
**Violation of the Comprehensive Computer Data Access and Fraud Act**
**Against Flo Health, Facebook, Google, and Flurry**
**Cal. Penal Code § 502**
**("CDAFA")**
**(On Behalf of Plaintiffs and the Class and Subclass)**

414. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

415. The California Legislature enacted the Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502 ("CDAFA") to "expand the degree of protection afforded. . . from tampering, interference, damage, and unauthorized access to ([including the extraction of data from)] lawfully created computer data and computer systems," finding and declaring that "the proliferation of computer technology has resulted in a concomitant proliferation of . . . forms of unauthorized access to computers, computer systems, and computer data," and that "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals. . . ." Cal. Penal Code § 502(a).

[89] Analysis of Proposed Consent Order to Aid Public Comment, *In the Matter of Flo Health, Inc.*, File No. 1923133 (Jan, 13, 2021), https://www.ftc.gov/system/files/documents/cases/flo_health_analysis.pdf.

416. Plaintiffs' and Class members' devices on which they utilized the Flo App, including their computers, smart phones, and tablets, constitute "computers, computer systems, and/or computer networks" within the meaning of the CDAFA. *Id.* § 502(b)(5).

417. Defendants Flo Health, Facebook, Google, and Flurry violated § 502(c)(1)(B) of the CDAFA by knowingly accessing without permission Plaintiffs' and Class members' devices in order to wrongfully obtain and use their personal data, including their intimate health data, in violation of Flo App users' reasonable expectations of privacy in their devices and data.

418. Defendants Flo Health, Facebook, Google, and Flurry violated Cal. Penal Code § 502(c)(2) by knowingly and without permission accessing, taking, copying, and using Plaintiffs' and the Class members' personally identifiable information, including their intimate health data.

419. The computers and mobile devices that Plaintiffs and Class members used to when accessing the Flo App all have and operate "computer services" within the meaning of the CDAFA. Facebook, Google, and Flurry violated §§ 502(c)(3) and (7) of the CDAFA by knowingly and without permission accessing and using those devices and computer services, and/or causing them to be accessed and used, *inter alia*, in connection with Flo Health's wrongful agreement to share such data with Facebook, Google, and Flurry, who in turn, where granted unauthorized and unfettered use of said data.

420. Defendant Flo Health violated §§ 502(c)(6) and (c)(13) of the CDAFA by knowingly and without permission by Plaintiffs and the Class, providing and/or assisting in providing Facebook, Google, and Flurry the ability to access Plaintiffs' and the Class members' private and intimate health data via the SDKs embedded into the Flo App.

421. Under § 502(b)(12) of the CDAFA a "Computer contaminant" is defined as "any set of computer instructions that are designed to . . . record, or transmit information within computer, computer system, or computer network without the intent or permission of the owner of the information." Defendants Flo Health, Facebook, Google, and Flurry violated § 502(c)(8) by knowingly and without permission introducing a computer contaminant via the SDKs embedded into the Flo App by Defendants Flo Health, Facebook, Google, and Flurry, which intercepted

Plaintiffs' and the Class members' private and intimate health data. As described *supra*, the embedded SDKs are deeply hidden; Plaintiffs and Class members had no way to remove them or opt out of their functionality.

422. Plaintiffs and Class members suffered damage and loss as a result of Defendants' conduct. Defendants' practices have deprived Plaintiffs and the Class members of control over their valuable property (namely, their sensitive personal data), the ability to receive compensation for that data, and the ability to withhold their data for sale.

423. Plaintiffs and the Class members seek compensatory damages in accordance with California Penal Code § 502(e)(1), in an amount to be proven at trial, and injunctive or other equitable relief.

424. Plaintiffs and Class members have also suffered irreparable and incalculable harm and injuries from Defendants' violations. The harm will continue unless Defendants Flo Health, Facebook, Google, and Flurry are enjoined from further violations of this section. Plaintiffs and Class members have no adequate remedy at law.

425. Plaintiffs and the Class members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Defendants Flo Health, Facebook, Google, and Flurry's violations were willful and, upon information and belief, those Defendants are guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294. Plaintiffs and the Class members are also entitled to recover their reasonable attorneys' fees under § 502(e)(2).

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs on behalf of themselves and the proposed Class respectfully request that the Court enter an order:

A. Certifying the Classes and appointing Plaintiffs as the Classes Representatives;

B. Finding that all the Defendants' conduct was unlawful, as alleged herein;

C. Awarding declaratory relief against all Defendants;

D. Awarding such injunctive and other equitable relief as the Court deems just and proper;

E. Awarding Plaintiffs and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

F. Awarding Plaintiffs and the Class members pre-judgment and post-judgment interest;

G. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses; and

H. Granting such other relief as the Court deems just and proper.

**DEMAND FOR JURY TRIAL**

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiffs demand a jury trial as to all issues triable by a jury.

Dated: September 2, 2021

/s/ *James M. Wagstaffe*

James M. Wagstaffe (95535)
Frank Busch (258288)
**WAGSTAFFE, VON LOEWENFELDT, BUSCH & RADWICK LLP**
100 Pine Street, Suite 725
San Francisco, CA 94111
Tel: (415) 357-8900
Fax: (415) 357-8910
wagstaffe@wvbrlaw.com
busch@wvbrlaw.com

*Counsel for Plaintiffs Erica Frasco and Sarah Wellman*

Carol C. Villegas (*pro hac vice*)
Michael P. Canty (*pro hac vice*)
Ross Kamhi (*pro hac vice*)
David Saldamando (*pro hac vice* pending)
**LABATON SUCHAROW LLP**
140 Broadway
New York, NY 10005
Tel: (212) 907-0700

Fax: (212) 818-0477
cvillegas@labaton.com
mcanty@labaton.com
rkamhi@labaton.com
dsaldamando@labaton.com

*Proposed Interim Co-Lead Counsel*
*for Plaintiffs and the Proposed Class*

Christian Levis (*pro hac vice*)
Amanda Fiorilla (*pro hac vice*)
**LOWEY DANNENBERG, P.C.**
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

*Proposed Interim Co-Lead Counsel*
*for Plaintiffs and the Proposed Class*

Diana J. Zinser (*pro hac vice*)
John A. Macoretta (*pro hac vice*)
Jeffrey L. Kodroff (*pro hac vice*)
**SPECTOR ROSEMAN & KODROFF, P.C.**
2001 Market Street, Suite 3420
Philadelphia, PA 19103
Tel: (215) 496-0300
Fax: (215) 496-6611
dzinser@srkattorneys.com
jmacoretta@srkattorneys.com
jkodroff@srkattorneys.com

*Proposed Interim Co-Lead Counsel*
*for Plaintiffs and the Proposed Class*

**LAW OFFICES OF RONALD A. MARRON**
RONALD A. MARRON (CA Bar 175650)
ron@consumersadvocates.com
ALEXIS M. WOOD (CA Bar 270200)
alexis@consumersadvocates.com
KAS L. GALLUCCI (CA Bar 288709)
kas@consumersadvocates.com
651 Arroyo Drive
San Diego, CA 92103

Tel: (619) 696-9006
Fax: (619) 564-6665

*Counsel for Plaintiffs Jennifer Chen and Tesha Gamino*

Kent Morgan Williams (*pro hac vice*)
**WILLIAMS LAW FIRM**
1632 Homestead Trail
Long Lake, MN 55356
Tel: (612) 940-4452
williamslawmn@gmail.com

Michael E. Jacobs (*pro hac vice*)
**HINKLE SHANOR LLP**
P.O. Box 2068
Santa Fe, NM 87504
Tel: (505) 982-4554
mjacobs@hinklelawfirm.com

William Darryl Harris, II (*pro hac vice*)
**HARRIS LEGAL ADVISORS LLC**
605 N High Street
Suite 146
Columbus, OH 43215
Tel: (614) 504-3350
Fax: (614) 340-1940
will@harrislegaladvisors.com

*Counsel for Plaintiffs Leah Ridgway and Autumn Meigs*