

BURSOR & FISHER, P.A.

L. Timothy Fisher (State Bar No. 191626)

Julia K. Venditti (State Bar No. 332688)

Joshua R. Wilner (State Bar No. 353949)

1990 North California Blvd., 9th Floor

Walnut Creek, CA 94596

Telephone: (925) 300-4455

Facsimile: (925) 407-2700

E-mail: ltfisher@bursor.com

jvenditti@bursor.com

jwilner@bursor.com

Attorneys for Plaintiff and the Putative Class

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

JANICE ADAM, individually and on behalf of
all others similarly situated,

Plaintiff,

v.

CARINGBRIDGE, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1 Plaintiff Janice Adam (“Plaintiff”) brings this action on behalf of herself and all others
2 similarly situated against CaringBridge, Inc. (“Defendant” or “CaringBridge”). Plaintiff makes the
3 following allegations pursuant to the investigation of herself counsel and upon information and
4 belief, except as to allegations specifically pertaining to herself and her counsel, which are based
5 on personal knowledge.

6 **NATURE OF THE ACTION**

7 1. This is a putative class action lawsuit brought against Defendant for aiding and
8 employing third parties—Google, LLC (“Google”) and Meta Platforms, Inc. (“Meta”) (together
9 with Google, the “Third Parties”)—to intercept, in real time, sensitive and confidential
10 communications and health information sent to and/or received by Plaintiff and putative class
11 members through Defendant’s website, caringbridge.org (the “Website”).

12 2. Specifically, Defendant owns and operates the CaringBridge Website, which is a
13 social media platform that purports to provide caregivers and individuals with “tools to share and
14 document a health journey, simplify care coordination, and connect caregivers with a supportive
15 community” (the “Platform”).¹ The Website allows consumers to share and document a health
16 journey, simplify care coordination, and connect caregivers with a supportive community (the use
17 of Defendant’s social media platform through the Website is referred to herein as the
18 “CaringBridge Service”).

19 3. On its Website, CaringBridge claims to offer the ability to “communicate to
20 everyone all at once in a safe and private space”² and advertises that its platform is a “safe place for
21
22
23
24
25
26

27 ¹ CaringBridge, *About us*, caringbridge.org/about-us.

28 ² *Id.*

1 health journeys”³ and a “trusted place to communicate[.]”⁴

2 4. To create an account, individuals must disclose their health condition to
3 CaringBridge through a drop-down menu that includes options such as “Brain Cancer,”
4 “HIV/AIDS,” “Substance Use Disorder,” and more.

5 5. Additionally, given the nature of the CaringBridge Service, consumers use the
6 Website to regularly their share confidential and sensitive personal and medical information with
7 other select users that they know in real life and with whom such users have specifically chosen to
8 disclose their confidential and sensitive information. Users who share their personal and medical
9 information through the CaringBridge Service do not intend to disclose such information broadly
10 or publicly, but only to these select other users.

11 6. However, the confidential medical information provided by users to Defendant at
12 the point of account creation, and confidential communications shared by users of the Website
13 thereafter through the CaringBridge Service, is surreptitiously intercepted in real time by Google
14 and Meta through their tracking technologies, as detailed below. Google and Meta are separate and
15 distinct third-party entities from the parties to these communications (*i.e.*, Defendant, as the entity
16 offering the CaringBridge Service, and Plaintiff and similarly situated consumers who created an
17 account through Defendant’s website and used the CaringBridge Service). The communications
18 input into the Website are surreptitiously intercepted, stored, and aggregated by Google and Meta
19 and used by Google and Meta for their own business purposes.

20 7. Thus, Defendant aids, employs, agrees, and conspires with Google and Meta to
21 intercept the confidential communications sent and received by consumers the Website and

22 ³ <https://apps.apple.com/us/app/caringbridge/id365726944> (description of CaringBridge mobile
23 application in iOS App Store); *see also id.* (“[CaringBridge] offers tools to share and document a
24 health journey, simplify care coordination, and connect caregivers with a supportive community.
25 CaringBridge addresses feelings of overwhelm, isolation, and loneliness by improving emotional
26 health and social connectedness, helping people come together in support of healing. With over
27 300,000 people on the platform every day sending or receiving support, there are over 1,600
28 messages of love, hope, and compassion posted every hour. And every 12 minutes a new
CaringBridge page is started. ... [CaringBridge is a] **trusted, private, and ad-free space** that ...
can provide to support family caregivers and their loved ones on a health journey. ...
[CaringBridge allows users to c]ommunicate to everyone all at once in a **safe and private space**,
relieving the burden of individually updating people.”) (emphasis added).

⁴ <https://www.caringbridge.org/>.

1 CaringBridge Service, including communications concerning sensitive personal and medical
2 information.

3 8. Plaintiff is a California citizen and resident who have accessed and used
4 Defendant's Website while in California and who, in the course of creating an account on the
5 Website and/or using the CaringBridge Service, inputted sensitive medical and personally
6 identifying information that was intercepted in real time by Google and Meta, the third parties that
7 Defendant aided and employed to wiretap on its Website. Plaintiff was not informed at any point
8 that third parties would have access to or collect and store the information she provided to
9 Defendant in connection with the CaringBridge Service. Instead, Plaintiff reasonably believed that
10 the personal information shared during the account creation process was only being shared with
11 Defendant, and that any sensitive information subsequently shared through Defendant's social
12 media Platform was only being shared with Defendant and those select other users of the
13 CaringBridge Service who were specifically chosen to receive such information by Plaintiff (*i.e.*,
14 Plaintiff's personal connections).

15 9. At no point is any user of the Website, like Plaintiff, adequately appraised of the
16 wiretapping, nor are they provided sufficient opportunity to consent to it.

17 10. Crucially, neither Defendant nor the Third Parties procured the consent of any
18 person who created an account on Website or shared personal information while using the
19 CaringBridge Service prior to the Third Parties' recording, accessing, reading, and learning of the
20 contents of Californians users' communications to Defendant through the Website and
21 CaringBridge Service. This is despite the Third Parties having the capability to use the contents of
22 those communications for purposes other than simply providing a copy to Defendant.

23 11. Accordingly, Plaintiff brings this action individually and on behalf of all others
24 similarly situated based on Defendants' unlawful conduct, seeking damages, restitution,
25 declaratory relief, injunctive relief, and reasonable attorneys' fees and costs, for: (1) violation of
26 the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 631(a); (2) invasion of privacy
27 under California's Constitution / intrusion upon seclusion; and (3) violation of the Electronic
28 Communications Privacy Act, 18 U.S.C. §§ 2511(1), *et seq.*

THE PARTIES

12. Plaintiff Janice Adam is a natural person and citizen of California, residing in Castro Valley, California, who created an account on the Website while in California in 2023, and who, in the course of doing so, input sensitive medical and personally identifying information that was intercepted in real time by the Third Parties that Defendant aided and employed to wiretap on its Website. Further, Plaintiff visited the Website and used the CaringBridge Service several times in 2023 while in California, to interact with family members and receive status updates on the health condition of her loved one. Once again, in doing so, Plaintiff provided sensitive medical and personally identifying information. As discussed in further detail below, that information was intercepted as it was entered into the Website by the Google and Meta, the third party entities that Defendant aided, agreed with, and employed to surreptitiously intercept Plaintiff's confidential communications to use for its own marketing, advertising, and analytics purposes. Plaintiff did not consent to—nor was she ever made aware of—the surreptitious interception and use of this personal information by the Third Parties. By failing to receive the requisite consent, Defendant breached its duties of confidentiality to Plaintiff. Plaintiff did not discover that her confidential communications were intercepted until January 2025.

13. CaringBridge, Inc. ("Caring Bridge") is a nonprofit organization registered in Minnesota, with its headquarters and principal place of business located at 1715 Yankee Doodle Road, No. 301, Eagan, Minnesota 55121. At all times relevant to the allegations herein, Defendant has owned and operated the Website and CaringBridge Service provided on the CaringBridge Platform, which it has offered and marketed to consumers in California and throughout the United States. Defendant provides its CaringBridge Service and Platform in California and has done business in and throughout California and throughout the United States at all times during the Class Period. Relevant to Plaintiff's claims herein, Defendant has, at all relevant times, offered the CaringBridge Service to consumers through the Website, whereby consumers must, in the course of creating an account on the Platform and/or using the CaringBridge Service, input sensitive medical and personally identifying information in order to share and document their health journeys with loved ones, simplify care coordination, and connect caregivers with a supportive

1 community. At all relevant times, acting alone or in concert with others, Defendant formulated,
2 directed, controlled, had the authority to control, and/or participated in the acts and practices set
3 forth in this Complaint.

4 **JURISDICTION AND VENUE**

5 14. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A), as
6 amended by the Class Action Fairness Act of 2005 (“CAFA”), because this case is a class action
7 where the aggregate claims of all members of the proposed class are in excess of \$5,000,000,
8 exclusive of interest and costs, there are more than 100 class members, and at least one member of
9 the proposed class is a citizen of a state different from at least one Defendant.

10 15. This Court has personal jurisdiction over Defendant because Defendant has, at all
11 times relevant hereto, systematically and continually conducted, and continues to conduct, business
12 in California, including within this District. Indeed, at all relevant times, Defendant has targeted
13 the California consumer market by, *inter alia*, deliberately offering and marketing the Website and
14 the CaringBridge Service to consumers in California. Defendant has therefore intentionally availed
15 itself of the benefits and privileges of the California consumer market through the promotion,
16 marketing, and sale of its products and/or services to residents within California, including within
17 this District, such that it should reasonably expect to be brought into court in this State and District
18 as a result of its activities here.

19 16. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a
20 substantial portion of the events, omissions, and acts giving rise to Plaintiff’s claims occurred in
21 this District. Moreover, Defendant systematically conducts business in this District and throughout
22 the State of California, and Plaintiff resides in this District.

23 **FACTUAL ALLEGATIONS**

24 **I. Background On The California Information Privacy Act (“CIPA”)**

25 17. The California Legislature enacted the CIPA to protect certain privacy rights of
26 California citizens. The California Legislature expressly recognized that “the development of new
27 devices and techniques for the purpose of eavesdropping upon private communications ... has
28 created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free

1 and civilized society.” Cal. Pen. Code § 630.

2 18. As the California Supreme Court has held in explaining the legislative purpose
3 behind CIPA:

4 While one who imparts private information risks the betrayal of his
5 confidence by the other party, a substantial distinction has been
6 recognized between the secondhand repetition of the contents of a
7 conversation and its *simultaneous dissemination to an unannounced
second auditor, whether that auditor be a person or mechanical
device.*

8 As one commentator has noted, such secret monitoring denies the
9 speaker an important aspect of privacy of communication—*the right
to control the nature and extent of the firsthand dissemination of his
statements.*

10 *Ribas v. Clark*, 38 Cal. 3d 355, 360-61 (1985) (emphasis added; internal citations omitted).

11 19. As part of CIPA, the California Legislature enacted § 631(a), which prohibits, in
12 relevant part, any person or entity from: (1) “willfully and without the consent of all parties to the
13 communication ... read[ing], or attempt[ing] to read, or to learn the contents or meaning of any . . .
14 communication while the same is in transit or passing over any wire, line, or cable, or is being sent
15 from, or received at any place within [California]”; or (2) “us[ing], or attempt[ing] to use, in any
16 manner, or for any purpose, or to communicate in any way, any information so obtained[.]” Cal.
17 Pen. Code § 631(a).

18 20. CIPA § 631(a) also penalizes [iv] those who “aid[], agree[] with, employ[], or
19 conspire[] with any person” who conducts the aforementioned violations, or those who “permit”
20 the violations. Cal. Pen. Code § 631(a).

21 21. Notably, CIPA § 631(a)’s applicability is not limited to phone lines, but also applies
22 to “new technologies” such as computers, the internet, and email. *See Matera v. Google, Inc.*,
23 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new technologies” and
24 must be construed broadly to effectuate its remedial purpose of protecting privacy); *Javier v.*
25 *Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) (“Though written in terms of
26 wiretapping, Section 631(a) applies to Internet communications.”); *In re Facebook, Inc. Internet*
27 *Tracking Litig.*, 956 F. 3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law
28

1 privacy claims based on Facebook’s collection of internet browsing history).

2 22. CIPA § 631(a) requires consent to an interception to occur *before* the interception
3 itself occurs, not after. *See Javier*, 2022 WL 1744107, at *2 (“[W]e conclude that the California
4 Supreme Court would interpret Section 631(a) to require the prior consent of all parties to a
5 communication.”); see also *Ribas*, 38 Cal. 3d at 361 (“The Privacy Act has been read to require the
6 assent of all parties to a communication *before another may listen.*”) (emphasis added).

7 23. Individuals may bring an action against the violator of any provision of the CIPA
8 for injunctive relief and statutory damages equal to \$5,000 per violation. *See* Cal. Pen. Code §
9 637.2(a)(1). Plaintiff does so, here, against Defendant.

10 II. DEFENDANT VIOLATES THE CIPA

11 24. CaringBridge is a social media platform that purports to provide caregivers and
12 individuals with “tools to share and document a health journey, simplify care coordination, and
13 connect caregivers with a supportive community.”⁵

14 25. On its Website, CaringBridge claims to offer the ability to “communicate to
15 everyone all at once in a safe and private space”⁶ and advertises that its platform is a “safe place for
16 health journeys”⁷ and a “trusted place to communicate[.]”⁸

17 26. To create an account, individuals must disclose their health condition to
18 CaringBridge through a drop-down menu that includes options such as “Brain Cancer,”
19 “HIV/AIDS,” “Substance Use Disorder,” and more.

20 _____
21 ⁵ CaringBridge, *About us*, [caringbridge.org/about-us](https://www.caringbridge.org/about-us).

22 ⁶ *Id.*

23 ⁷ <https://apps.apple.com/us/app/caringbridge/id365726944> (description of CaringBridge mobile
24 application in iOS App Store); *see also id.* (“[CaringBridge] offers tools to share and document a
25 health journey, simplify care coordination, and connect caregivers with a supportive community.
26 CaringBridge addresses feelings of overwhelm, isolation, and loneliness by improving emotional
27 health and social connectedness, helping people come together in support of healing. With over
28 300,000 people on the platform every day sending or receiving support, there are over 1,600
messages of love, hope, and compassion posted every hour. And every 12 minutes a new
CaringBridge page is started. ... [CaringBridge is a] **trusted, private, and ad-free space** that ...
can provide to support family caregivers and their loved ones on a health journey. ...
[CaringBridge allows users to c]ommunicate to everyone all at once in a **safe and private space**,
relieving the burden of individually updating people.”) (emphasis added).

⁸ <https://www.caringbridge.org/>.

27. Among the features provided on the Website are the ability to share updates in the form of messages and photos, link to resources such as GoFundMe and MealTrain pages, and accept gift cards or grocery delivery support.

III. The Third Party Wiretappers

28. As noted above, Defendant aids and employs separate and distinct third parties—Google, LLC (“Google”) and Meta Platforms, Inc. (“Meta”) (together with Google, the “Third Parties”)—to intercept, in real time, sensitive and confidential communications and medical and personally identifying information sent to and/or received by Plaintiff and putative class members through the Website and CaringBridge Service. As explained in detail below, Google and Meta, neither of which are parties to the communications at issue (*i.e.*, Defendant, as the entity offering the CaringBridge Service, and Plaintiff and similarly situated consumers who created an account through Defendant’s website and used the CaringBridge Service), use tracking technologies to surreptitiously intercept Plaintiff’s and class members’ confidential communications, and they also store and aggregate the sensitive consumer information intercepted so that they may use such information for their own business purposes. These tools, along with any other tracking software or devices that Google and Meta may deploy on their partners’ websites, are collectively referred to herein as the “Services.”

A. Google Analytics’ Tracking Code

29. The Google Analytics tracking code is a piece of code that can be installed into websites to track page visits, button clicks, text entered into websites, and other actions taken by website visitors. The tracking code is connected to the Google Analytics platform.

30. According to Google, “Google Analytics is a platform that collects data from [] websites and apps to create reports that provide insights into [] business[es].”⁹ Google describes these reports and insights as follows:¹⁰

⁹ GOOGLE, HOW GOOGLE ANALYTICS WORKS, <https://support.google.com/analytics/answer/12159447>.

¹⁰ GOOGLE, ANALYTICS FEATURES, <https://marketingplatform.google.com/about/analytics/features/>.

Real-Time Reporting

- Monitor activity on your site or app as it happens.

Acquisition Reports

- See how users land on your site or app and understand the effectiveness of your marketing.
 - User Acquisition[:]
Discover how users reach your site or app through different paid and organic sources.
 - Traffic Acquisition[:]
See a session-based view of traffic and engagement on your site or app through different paid and organic traffic sources.

Engagement Reports

- Better understand what content drives engagement and conversions on your site or app.
 - Events Report[:]
Get a detailed view of user actions, system events, or errors.
 - Conversion Report[:]
See how all your marketing channels are working together to drive conversions.
 - Pages and Screen Report[:]
See which web pages and app screens users engage with the most.

Monetization Reports

- See how much revenue your site or app generates whether it's from ecommerce, subscriptions, or ads.
 - Ecommerce[:]
Analyze purchase activity including product and transaction information, average purchase revenue, average purchase revenue per user, and other data.
 - In-App Purchases[:]
Improve your app monetization with insights about the highest performing products and subscriptions.
 - Publisher Ads[:]
See ad revenue that your app generates using the Google Analytics for Firebase SDK.

31. This gathered information is used for marketing and advertising. Specifically, Google “Analytics is designed to work seamlessly with other Google solutions and partner products” and can “unlock deeper insights into [advertising] campaign performance from Google Ads, Display & Video 360, and Search Ads 360.”¹¹ Google Analytics integrates with Google Ads so that clients, like Defendant, can “[s]ee [] Ads data together with [] website and app performance data in the Google Ads reports in Analytics.”¹² Google Analytics integrates with Display & Video

¹¹ *Id.*

¹² *Id.*

360 and Search Ads so that clients, like Defendant, can “[e]xport conversions created in Analytics[,]” “create audiences that are predicted to take [certain] actions[,]” and “use them for automated bidding” in Display & Video 360 and Search Ads.¹³

32. Gathered information is also used for analytics. With Google Analytics, clients, like Defendant, can “apply[] Google’s machine learning models, . . . analyze [] data[,] and predict future actions people may take, like making a purchase or churning.”¹⁴ Additionally, Google Analytics can “automatically detect and surface actionable insights from [gathered] data like important changes, new trends, and other growth opportunities[.]”¹⁵ And Google can provide “[a]nswers to [marketers’ q]uestions . . . in natural language[,] . . . to quickly find [] metric[s], report[s], or insights[.]”¹⁶ Through Google Analytics’ “[u]ser [e]xploration” functions, it is even possible to “[s]elect specific groups of users and drill down deeper to understand how those users engage with [a] site or app.”¹⁷

33. Thus, Google Analytics furnishes “a complete understanding of [] customers across devices and platforms[,] . . . [and] gives [] the tools[] . . . to understand customer journey and improve marketing ROI.”¹⁸

34. As such, Google has the capacity to use the information intercepted from the Website for its own purposes, assembling the data collected into Similar Audiences and other datasets to target users with advertising.

35. In addition to personally identifying information entered into websites, Google receives additional identifying information, including but not limited to the users’ IP address, device information, and User-IDs.

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ GOOGLE, ANALYTICS OVERVIEW, <https://marketingplatform.google.com/about/analytics/>.

1 36. For example, the Website utilizes Google’s “cid” or “Client ID” function to identify
2 users as they navigate the Website.

3 37. In addition to User-IDs, upon receiving information from the Website, Google also
4 utilizes a “browser-fingerprint” to personally identify consumers. A browser-fingerprint is
5 information collected about a computing device that is used to identify the specific device.

6 38. These browser-fingerprints are used to uniquely identify individual users when a
7 computing device’s IP address is hidden or cookies are blocked and can provide a wide variety of
8 data.

9 39. As Google explained, “[w]ith fingerprinting, developers have found ways to use
10 tiny bits of information that vary between users, such as what device they have or what fonts they
11 have installed to generate a unique identifier which can then be used to match a user across
12 websites.”

13 40. The value of browser-fingerprinting to advertisers (and trackers who want to
14 monetize aggregated data) is that they can be used to track website users just as cookies do, but it
15 employs much more subtle techniques. Additionally, unlike cookies, users cannot clear their
16 fingerprint and therefore cannot control how their personal information is collected.

17 41. In 2017, researchers demonstrated that browser fingerprinting techniques can
18 successfully identify 99.24 percent of all users.

19 42. Browser-fingerprints are personal identifiers. Tracking technologies, like the ones
20 developed by Google and utilized on the Website, can collect browser-fingerprints from website
21 visitors

22 43. Defendant intentionally embedded and configured Google Analytics on all pages of
23 its Website.

24 44. Each time a user creates a CaringBridge account and discloses their medical
25 condition, the Google Analytics tracking code automatically sends a simultaneous transmission of
26 that information to Google, and shown in the image below.

```

v      2
tid    G-E2WFJTZLTL
gtm    45je4cc1v9173696364z89135160797za200zb9135160797
_p     1736176539748
gcd    1313131111
npa    0
dma    0
tag_exp 101925629~102067555~102067808~102081485~102198178
cid    1676291313.1736176540
ul     en-us
sr     3072x1728
uaa    x86
uab    64
uafvl
Google%2520Chrome%3B131.0.6778.205%7CChromium%3B131.0.6778.205%7CNot_A%2520Brand%3
B24.0.0.0
uamb   0
uam
uap    Windows
uapv   15.0.0
uaw    0
are    1
pae    1
frm    0
pscdl  noapi
_s     16
dl
https%3A%2F%2Fwww.caringbridge.org%2Fsite%2Ffe8fd37b5-cc41-11ef-b83d-231c27022f73%3Fshare
%3D1
uid    718ed6eb-cc41-11ef-a3c2-ffd6099d69a5
sid    1736176540
sct    1
seg    1
dr     https%3A%2F%2Fwww.caringbridge.org%2Fstart
dt
en     ucla_survey_interaction
ep.userIdDimension 718ed6eb-cc41-11ef-a3c2-ffd6099d69a5
ep.content_group   Other
ep.event_action    DISPLAY
ep.health_condition BREAST_CANCER
ep.last_post_date  01%2F06%2F2025
epn.posts_on_site  1
ep.site_creation_date 01%2F06%2F2025
ep.site_id         e8fd37b5-cc41-11ef-b83d-231c27022f73
ep.userRole        Author
epn.visits         1
ep.isPatient       true
epn.days_without_post 0
_et             976
tfd             365815

```

45. Google intercepted this type of confidential information from Plaintiff and Class Members in real time as the information was entered into the Website. Google then viewed each

1 and every piece of intercepted information, processed it, and assembled it for use in the advertising
2 services detailed above.

3 46. Google also collects information sufficient to identify each users, such as that user's
4 IP address, geolocation, browser, operating system, device information, and Wi-Fi provider and
5 router information.

6 47. The purpose of this invasion of privacy is straightforward: Google collects
7 information from Defendant's website and sends back an analysis of that information, identifying
8 website traffic and ad performance and targeting ads for specific individuals.

9 48. This is valuable to Defendant because it improves the effectiveness of Defendant's
10 advertisements, allows for the targeting of users, and provides performance information for ad
11 campaigns.

12 49. In addition to helping companies like Defendant make better use of their own
13 customer information, Google aggregates that information with the information collected from all
14 sites containing the Google Analytics Pixel to track users across multiple websites and platforms,
15 which increases the value of Google's advertising services when they are offered to other
16 companies.

17 50. Thus, the agreement for Defendant to aid in Google's wiretapping of Plaintiff and
18 Class Members' confidential information is done for the purpose of improperly increasing the
19 advertising efficiency and, by extension, profits of both parties.

20 **B. The Meta Tracking Pixel**

21 51. Meta Platforms, Inc. ("Meta"), formerly known as Facebook, Inc., owns and
22 operates "Facebook," which is the largest social networking site on the planet, touting 2.9 billion
23 monthly active users.¹⁹ Facebook describes itself as a "real identity platform,"²⁰ meaning users are

24
25 ¹⁹ Sean Burch, *Facebook Climbs to 2.9 Billion Users, Report 29.1 Billion in Q2 Sales*, YAHOO!
(July 28, 2021), available [https://www.yahoo.com/now/facebook-climbs-2-9-billion-](https://www.yahoo.com/now/facebook-climbs-2-9-billion-202044267.html)
26 [202044267.html](https://www.yahoo.com/now/facebook-climbs-2-9-billion-202044267.html) (last accessed June 21, 2024).

27 ²⁰ Sam Schechner & Jeff Horowitz, *How Many Users Does Facebook Have? The Company*
Struggles to Figure it Out, Wall St. J. (Oct. 21, 2021) available [https://www.wsj.com/articles/how-](https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701)
28 [many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701](https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701) (last
accessed June 21, 2024).

1 allowed only one account and are encouraged to share “the name they go by in everyday life.”²¹
 2 To that end, when creating an account, users provide their first and last name, along with their
 3 birthday, gender, and phone number or email address.²²

4 52. Meta generates revenue by selling advertising space on Facebook, and other social
 5 media platforms or mobile applications that it also owns, like Instagram.²³

6 53. Meta sells advertising space by highlighting its ability to target users.²⁴ Meta can
 7 target users effectively because it surveils user activity both on and off its site.²⁵ This allows Meta
 8 to make inferences about users beyond what they explicitly disclose, like their “interests,”
 9 “location,” and “demographics.”²⁶ Meta compiles this information into a generalized dataset called
 10 “Core Audiences,” which advertisers use to apply highly specific filters and parameters for their
 11 targeted advertisements.²⁷

12 54. Businesses can also build “Custom Audiences.”²⁸ Custom Audiences enable
 13 businesses to reach “people who already know [their] business,” because Meta can track whether
 14 they’re loyal customers or people who have used a particular business’ app or visited their
 15 website.²⁹ Businesses can use Custom Audiences to target existing customers directly, or they can

16
 17 ²¹ META, *Community Standards, Part IV Integrity and Authenticity*, available
https://www.facebook.com/communitystandards/integrity_authenticity (last accessed June 21,
 18 2024).

19 ²² META, *Sign Up*, available <https://www.facebook.com/> (last accessed June 21, 2024).

20 ²³ Mike Isaac, *Facebook Profit Surges 101 Percent on Strong Ad Sales*, N.Y. TIMES (July 28,
 2021) available <https://www.nytimes.com/2021/07/28/business/facebook-q2-earnings.html> (last
 21 accessed June 21, 2024).

22 ²⁴ META, *Why Advertise on Facebook, Instagram and other Meta Technologies*, available
<https://www.facebook.com/business/help/205029060038706> (last accessed June 21, 2024).

23 ²⁵ META, *About Meta Pixel*, available
<https://www.facebook.com/business/help/742478679120153?id=1205376682832142> (last accessed
 24 June 21, 2024).

25 ²⁶ META, *Audience Ad Targeting*, available <https://www.facebook.com/business/ads/ad-targeting>
 26 (last accessed June 21, 2024).

27 ²⁷ META, *Easier, More Effective Ways to Reach the Right People on Facebook*, available
<https://www.facebook.com/business/news/Core-Audiences> (last accessed June 21, 2024).

28 ²⁸ META, *Create a website custom audience*, available
<https://www.facebook.com/business/help/1474662202748341?id=2469097953376494> (last
 accessed June 21, 2024).

²⁹ META, *Audience ad targeting*, available <https://en-gb.facebook.com/business/ads/ad-targeting>
 (last accessed June 21, 2024).

1 use it to build “Lookalike Audiences,” which “leverage[] information such as demographics,
 2 interests, and behaviors from your source audience to find new people who share similar
 3 qualities.”³⁰ Unlike Core Audiences, Custom Audiences require an advertiser to supply the
 4 underlying data to Meta. They can do so through two mechanisms: by manually uploading contact
 5 information for customers, or by utilizing Facebook’s “Business Tools,” which collect and transmit
 6 the data automatically.³¹ One such Business Tool is the Meta Pixel.

7 55. The Meta Pixel is a piece of code that businesses, like Defendant, can integrate into
 8 their Website. Once activated, the Meta Pixel “allows [the site] to track visitor activity on [their]
 9 website.”³² When the Meta Pixel captures an action, it sends a record to Facebook. Once this
 10 record is received, Meta processes it, analyzes it, and assimilates it into datasets like the Core
 11 Audiences and Custom Audiences.

12 56. Businesses control what actions – or, as Meta calls it, “events” – the Meta Pixel will
 13 collect on that business’s site, including the website’s metadata, along with what pages a consumer
 14 views.³³ Businesses can also configure the Meta Pixel to track other events. Meta offers a menu of
 15 “standard events” from which businesses can choose to track, including what content a consumer
 16
 17
 18
 19

20 ³⁰ META, *About Lookalike Audiences*,
 21 <https://www.facebook.com/business/help/164749007013531?id=401668390442328> (last accessed
 22 June 21, 2024).

23 ³¹ META, *Create a Customer List Custom Audience*, available
 24 <https://www.facebook.com/business/help/170456843145568?id=2469097953376494>; *See Also*
 25 *Meta, Create a Website Custom Audience*, available
 26 <https://www.facebook.com/business/help/1474662202748341?id=2469097953376494> (last
 27 accessed June 21, 2024).

28 ³² META, *Meta Pixel*, available <https://developers.facebook.com/docs/meta-pixel/> (last accessed
 June 21, 2024).

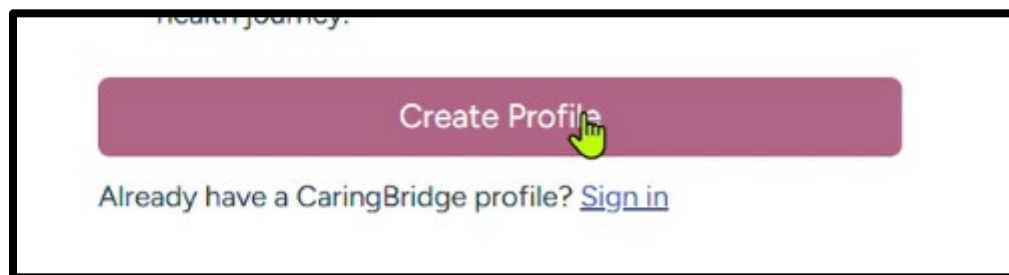
³³ *See* META, *Meta Pixel, Accurate Event Tracking, Advanced*, available
<https://developers.facebook.com/docs/facebook-pixel/advanced/>; *See also* Facebook, *Best Practices*
for Facebook Pixel Setup,
<https://www.facebook.com/business/help/218844828315224?id=1205376682832142> (last accessed
 June 21, 2024).

views or purchases.³⁴ An advertiser can also create their own tracking parameters by building a “custom event.”³⁵

57. Likewise, businesses using the pixel on their website control how the Meta Pixel identifies consumers. The Meta Pixel is configured to automatically collect “HTTP Headers” and “Pixel-specific Data.”³⁶ The HTTP Headers collect “IP addresses, information about the web browser, page location, document referrer and persons using the website.”³⁷ Pixel-specific Data includes “the Pixel ID and Cookie.”³⁸

58. The Meta Pixel, like website cookies generally, attaches to the browser that the user uses to access their Facebook account. That cookie then follows the user’s web activity occurring within that same browser. For example, if the user accesses Facebook.com through their Safari browser, then moves to reelshort.com after leaving Facebook, the Meta Pixel will continue to track that user’s activity on that browser.

59. Unbeknownst to Website users, Defendant knowingly discloses users’ confidential information and confidential health information to Meta. For example, as shown in the figure below, the Meta Pixel intercepts “button click” events showing that users took certain actions on the website. For example, Meta receives an event when a user creates a profile.



³⁴ META, *Specifications for Facebook Pixel Standard Events*, <https://www.facebook.com/business/help/402791146561655?id=1205376682832142> (last accessed June 21, 2024).

³⁵ META, *About Standard and Custom Website Events*, <https://www.facebook.com/business/help/964258670337005?id=1205376682832142> (last accessed June 21, 2024).

³⁶ META, *Meta Pixel*, <https://developers.facebook.com/docs/facebook-pixel/> (last accessed June 21, 2024).

³⁷ *Id.*

³⁸ *Id.*

```

id      1718196178206916
ev      SubscribedButtonClick
dl      https%3A%2F%2Fwww.caringbridge.org%2Fprofile%2Fregister%3Ffrom%3D1
rl
if      false
ts      1736176627310
cd[buttonFeatures]
%7B%22classList%22%3A%22button%20primary%20fullWidth%20hideOutlineForMouse%20jsx-bbc8723
b0062cfc9%22%2C%22destination%22%3A%22https%3A%2F%2Fwww.caringbridge.org%2Fprofile%2F
register%3Ffrom%3D1%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22inn
erText%22%3A%22Create%20Profile%22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22
button%22%2C%22type%22%3A%22submit%22%2C%22name%22%3A%22%22%2C%22value%22%3
A%22%22%7D
cd[buttonText].Create%20Profile

```

60. Moreover, when a user navigates to a page on the Website, the Meta Pixel first generates a PageView event that discloses the webpage's Universal Resource Locator ("URL") containing the page that the consumer has requested and viewed. When the user enters their email address, that information is disclosed to Meta in the URL.

```

https://www.facebook.com/tr/?
id      1718196178206916
ev      PageView
dl      https%3A%2F%2Fwww.caringbridge.org%2Fprofile%2Fregister%2Fconfirm%3Femail%3Dthommy5431%
2540yahoo.com
if      false
ts      1736176628300
sw      3072
sh      1728
udf[fn] fc5a299cd8cd644f40bdcc8f7ae00e89a4ae4fbc44031c4bc27e54dd4bcb9773
udf[ln] c1d35cc3471fe509203d85b3e7a53fc82337ac9ae2c797b838621f706fe37df8
udf[em] 2a9a22d88b031064ea86ff104d1cabf8b14a866c2a4adf136def1330b49fecbb
v      2.9.179
r      stable
a      tmSimo-GTM-WebTemplate
ec      6
o      6174
fbp     fb.1.1736176540495.133593818595341685
ler     empty
cdl     API_unavailable
it      1736176540246
coo     false
rqm     GET

```

CLASS ALLEGATIONS

61. **Class Definition:** Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of themselves and other similarly situated individuals defined as follows:

All persons in the United States who, within the applicable statute of limitations period, up to and including the date of final judgment in this action, accessed and used the CaringBridge Service and had their confidential communications and/or sensitive medical or personally identifiable information collected and intercepted by a third party.

62. **California Subclass Definition:** Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of themselves and other similarly situated individuals defined as follows:

All persons in California who, within the applicable statute of limitations period, up to and including the date of final judgment in this action, accessed and used the CaringBridge Service and had their confidential communications and/or sensitive medical or personally identifiable information collected and intercepted by a third party.

63. The following people are excluded from the Class: (i) any Judge presiding over this action and members of his or her family; (ii) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliates, and any entity in which Defendant or its parents have a controlling interest (including current and former employees, officers, or directors); (iii) persons who properly execute and file a timely request for exclusion from the Class; and (iv) the legal representatives, successors, and assigns of any such excluded persons.

64. Plaintiff reserves the right to amend the definition of the Class if discovery or investigation reveals that the Class should be expanded or otherwise modified, and/or to add additional subclasses as necessary prior to filing a motion for class certification.

65. **Numerosity.** Members of the Classes are so numerous that joinder of all members would be unfeasible and not practicable. On information and belief, the Class comprises at least thousands of consumers throughout California. Moreover, the Class is ascertainable and identifiable from Defendant's records. The precise number of Class members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class members

1 may be notified of the pendency of this action by mail and/or publication through the distribution
2 records of Defendant.

3 **66. Commonality and Predominance.** There are well-defined common questions of
4 fact and law that exist as to all members of the Class and that predominate over any questions
5 affecting only individual members of the Class. These common legal and factual questions, which
6 do not vary between members of the Class, and which may be determined without reference to the
7 individual circumstances of any Class member, include, but are not limited to, the following: (a)
8 whether Defendant violated CIPA § 631; (b) whether Defendant aided, agreed with, and/or
9 employed third parties to collect, read and/or attempt to read, review, and/or record users'
10 communications and activities on the Website; (c) whether Defendant sought or obtained prior
11 consent—express or otherwise—from Plaintiff and the Class to the collection of their information
12 by third parties; (d) whether the information collected is capable of identifying users; and (e)
13 whether Plaintiff and members of the Class are entitled to actual and/or statutory damages for the
14 aforementioned violations

15 **67. Typicality.** The claims of the named Plaintiff is typical of the claims of the Class
16 because the named Plaintiff, like all other members of the Class members, is a California resident
17 who used Defendant's Website and CaringBridge Service and had their sensitive medical and/or
18 personal information intercepted by third parties, Google and Meta, without their prior consent or
19 knowledge. Plaintiff's claims are therefore based on the same legal theories as the claims of other
20 Class Members.

21 **68. Adequacy.** Plaintiff is an adequate representative of the Class because their
22 interests do not conflict with the interests of the Class members they seek to represent, they have
23 retained competent counsel experienced in prosecuting class actions, and they intend to prosecute
24 this action vigorously. The interests of members of the Class will be fairly and adequately
25 protected by Plaintiff and their counsel.

26 **69. Superiority.** The class mechanism is superior to other available means for the fair
27 and efficient adjudication of the claims of members of the Class. Each individual member of the
28 Class may lack the resources to undergo the burden and expense of individual prosecution of the

1 complex and extensive litigation necessary to establish Defendant’s liability. Individualized
 2 litigation increases the delay and expense to all parties and multiplies the burden on the judicial
 3 system presented by the complex legal and factual issues of this case. Individualized litigation also
 4 presents a potential for inconsistent or contradictory judgments. In contrast, the class action device
 5 presents far fewer management difficulties and provides the benefits of single adjudication,
 6 economy of scale, and comprehensive supervision by a single court on the issue of Defendant’s
 7 liability. Class treatment of the liability issues will ensure that all claims and claimants are before
 8 this Court for consistent adjudication of the liability issues.

9 70. Additionally, certification of the proposed Class is appropriate under Fed. R. Civ.
 10 Proc. 23(b)(2) because Defendant has acted on or refused to act on grounds generally applicable to
 11 the Class, making appropriate declaratory, injunctive, and equitable relief with respect to the
 12 Plaintiff and the Class as a whole.

13 71. Without a class action, Defendant will continue a course of action that will result in
 14 further injury to Plaintiff and members of the Class.

15 72. Based on the foregoing allegations, Plaintiff’s claims for relief include those set
 16 forth below.

17 **COUNT I**
 18 **Violation of the California Invasion of Privacy Act (“CIPA”),**
 19 **Cal. Penal Code § 631**
(On Behalf Of The California Subclass)

20 73. Plaintiff re-alleges and incorporate by reference every allegation set forth in the
 21 preceding paragraphs as though fully alleged in this Count.

22 74. Plaintiff brings this claim individually and on behalf of the members of the
 23 California Subclass against Defendant.

24 75. CIPA § 631(a) imposes liability for “distinct and mutually independent patters of
 25 conduct.” *Tavernetti v. Superior Court*, 22 Cal. 3d 187, 192-93 (1978).

26 76. To establish liability under CIPA § 631(a), a plaintiff need only establish that the
 27 defendant, “by means of any machine, instrument, contrivance, or in any other manner,” does any
 28 of the following:

Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,

Or

Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,

Or

Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,

Or

Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

Cal. Pen. Code § 631(a).

77. Google and Meta are third parties that provide Defendant with the Services on the CaringBridge Website involving use of a “machine, instrument, contrivance, or ... other manner” to engage in the prohibited conduct at issue here.

78. The following items constitute “machine[s], instrument[s], or contrivance[s]” under the CIPA, and even if they do not, Google Analytics, and the Meta Pixel fall under the broad catch-all category of “any other manner”:

- a. The computer codes and programs Google and Meta used to track Plaintiff’s and Class Members’ communications while they were navigating caringbridge.org;
- b. Plaintiff’s and Class Members’ browsers;
- c. Plaintiff’s and Class Members’ computing and mobile devices;
- d. Google’s and Meta’s web and ad servers;
- e. The web and ad-servers from which Google and Meta tracked and intercepted Plaintiff’s and Class Members’ communications while they were using a web browser to access or navigate caringbridge.org;
- f. The computer codes and programs used by Google and Meta to effectuate their tracking and interception of Plaintiff’s and Class Members’ communications while they were using a web browser to visit caringbridge.org; and

- 1 g. The plan Google and Meta carried out to effectuate their tracking and interception
2 of Plaintiff's and Class Members' communications while they were using a web
3 browser to visit caringbridge.org.

4 79. As described above, Google and Meta are "separate legal entit[ies] that offer[]
5 'software-as-a-service' and not merely a passive device." *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503,
6 520 (C.D. Cal. 2021). Accordingly, Google and Meta are third parties to any communications
7 through the Website between Plaintiff and Class Members on the one hand, and Defendant on the
8 other. *See id.* at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal.
9 2023); *Yockey v. Salesforce, Inc.*, --- F. Supp. 3d ---, 2024 WL 3875785, at *4 (N.D. Cal. Aug. 16,
10 2024); *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019).

11 80. Google and Meta are third party wiretappers because they each have the capability
12 to use the contents of conversations they collect through their Services for their own purposes,
13 other than simply furnishing a copy of the communications to Defendant. *See Javier*, 2649 F.
14 Supp. 3d at 900; *see also Yockey v. Salesforce, Inc.*, 2023 WL 5519323, at *4 (N.D. Cal. Aug. 25,
15 2023).

16 81. At all relevant times, Google and Meta, through their Services, violated CIPA §
17 631(a) by willfully and without the consent of all parties to the communication, or in any
18 unauthorized manner, reading or attempting to read or learn the contents of electronic
19 communications between Plaintiff and Class Members, on the one hand, and Defendant, on the
20 other hand, while the electronic communications were in transit or passing over any wire, line or
21 cable or were being sent from or received at any place within California.

22 82. Furthermore, at all relevant times, by contracting for the provision of Google's and
23 Meta's Services and allowing Google and Meta to access and intercept Plaintiff's and Class
24 Members' communications, Defendant violated CIPA § 631(a) by aiding, agreeing with,
25 employing, permitting, or otherwise enabling Google and Meta's unlawful wiretapping.

26 83. The patient communications and health information that Defendant transmitted
27 using Google Analytics, and the Meta Pixel, such as information regarding Plaintiff's health status
28 and search history, constituted confidential information.

84. Defendant failed to inform Plaintiff and Class Members at any point that: (i) third parties, Google and Meta, were accessing, storing, and using Plaintiff's communications with Defendant, (ii) third parties, Google and Meta, were tapping or otherwise making an unauthorized connection with respect to Plaintiff's internet communications using the Third Parties' Services, and (iii) the content of Plaintiff's confidential communications with Defendant were being recorded, collected, intercepted, and analyzed by third parties, Google and Meta, using their Services. Defendant therefore failed to procure Plaintiff's consent to the conduct at issue.

85. Accordingly, neither Plaintiff nor any Class Member provided their prior consent to the Third Parties' interception of their communications with Defendant, nor did Plaintiff and Class Members consent to Defendant's employment of the same.

86. Thus, as demonstrated hereinabove, Defendant violated CIPA by aiding and permitting third parties to receive users' confidential communications through the Website without users' consent.

87. Plaintiff and Class Members were in California when they accessed Defendant's Website and had their communications unlawfully intercepted, read, collected, and stored by Google and Meta.

88. Pursuant to Cal. Pen. Code § 637.2, Plaintiff and the Class Members have been injured by Defendant's violations of CIPA § 631(a), and seek, individually and on behalf of the Class, statutory damages of \$5,000 for each of Defendant's violations of CIPA § 631(a).

COUNT II

Invasion of Privacy Under California's Constitution / Intrusion Upon Seclusion (On Behalf Of The Class)

89. Plaintiff re-alleges and incorporates by reference every allegation set forth in the preceding paragraphs as though fully alleged in this Count.

90. Plaintiff brings this claim individually and on behalf of the members of the Class against Defendant.

91. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications; and (2) making personal decisions

1 and/or conducting personal activities without observation, intrusion or interference, including, but
 2 not limited to, the right to visit and interact with various internet sites without being subjected to
 3 wiretaps without Plaintiff's and the Class Members' knowledge or consent.

4 92. At all relevant times, by using Google Analytics and the Meta Pixel to record and
 5 communicate users' identifying information, alongside their confidential communications,
 6 Defendant intentionally invaded Plaintiff's and the Class Members' privacy rights under the
 7 California Constitution, as well as intruded upon Plaintiff's and the Class Members' seclusion.

8 93. Plaintiff and Class Members had a reasonable expectation that their
 9 communications, identities, health status, searches and other data would remain confidential, and
 10 that Defendant would not install wiretaps on caringbridge.org.

11 94. Plaintiff and Class Members did not authorize Defendant to record and transmit
 12 Plaintiff's and Class Members' confidential communications and personally identifiable
 13 information, including health information.

14 95. This invasion of privacy was serious in nature, scope, and impact because it related
 15 to patients' confidential communications regarding, *inter alia*, the medical condition for which they
 16 were seeking support. Moreover, it constituted an egregious breach of the societal norms
 17 underlying the privacy right.

18 96. Accordingly, Plaintiff and Class Members seek all relief available for invasion of
 19 privacy claims under California's Constitution and common law.

20 **COUNT III**
 21 **Violation of the Electronic Communications Privacy Act ("ECPA"),**
 22 **18 U.S.C. §§ 2511(1), *et seq.***
(On Behalf Of The Class)

23 97. Plaintiff re-alleges and incorporates by reference every allegation set forth in the
 24 preceding paragraphs as though fully alleged in this Count.

25 98. Plaintiff brings this claim individually and on behalf of the members of the Class
 26 against Defendant.

27 99. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional
 28 interception of the content of any electronic communication. 18 U.S.C. § 2511.

1 100. The ECPA protects both sending and the receipt of communications.

2 101. The ECPA, 18 U.S.C. § 2520(a) provides a private right of action to any person
3 whose wire or electronic communications are intercepted, disclosed, or intentionally used in
4 violation of Chapter 119.

5 102. The transmission of Plaintiff's website page visits and selections each qualify as a
6 "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

7 103. The transmission of this information between Plaintiff and Class Members and the
8 Website with which they chose to exchange communications is the "transfer of signs, signals,
9 writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire,
10 radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce"
11 and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

12 104. The ECPA defines "contents," when used with respect to electronic
13 communications, to "include[] any information concerning the substance, purport, or meaning of
14 that communication." 18 U.S.C. 18 U.S.C. § 2510(8).

15 105. The ECPA defines an interception as the "acquisition of the contents of any wire,
16 electronic, or oral communication through the use of any electronic, mechanical, or other device."
17 18 U.S.C. § 2510(4).

18 106. The ECPA defines "electronic, mechanical, or other device," as "any
19 device...which can be used to intercept a[n]...electronic communication." 18 U.S.C. § 2510(5).

20 107. The Google Pixel and the Meta Pixel constitute "devices" within the meaning of the
21 ECPA.

22 108. Plaintiff and Class Members' interactions with the Website are electronic
23 communications under the ECPA.

24 109. By utilizing the Google Pixel and the Meta Pixel, as described herein, Defendant
25 intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the
26 electronic communications of Plaintiff and Class members in violation of 18 U.S.C. § 2511(1)(a).

1 110. Defendant intercepted confidential information. This confidential information is
2 then added to consumer profiles and monetized for targeted advertising purposes, among other
3 things.

4 111. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class
5 Members' electronic communications, while knowing or having reason to know that the
6 information was obtained through the interception of an electronic communication in violation of
7 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

8 112. Defendant intentionally intercepted the contents of Plaintiff's and Class Members'
9 electronic communications for the purpose of committing a criminal or tortious act in violation of
10 the Constitution or laws of the United States or of any state, namely, invasion of privacy, intrusion
11 upon seclusion, CIPA, and other state wiretapping and data privacy laws, among others.

12 113. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that
13 intercepts or causes interception to escape liability if the communication is intercepted for the
14 purpose of committing any tortious or criminal act in violation of the Constitution or laws of the
15 United States or of any State. Here, as alleged above, "[t]he association of Plaintiff's data with
16 preexisting user profiles is a further use of Plaintiff's data that satisfies [the crime-tort] exception,"
17 because it "violate[s] state law, including the [CIPA], intrusion upon seclusion, and invasion of
18 privacy." *Brown v. Google, LLC*, 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021); *see also Marden*
19 *v. LMND Medical Group, Inc.*, 2024 WL 4448684, at *2 (N.D. Cal. July 3, 2024); *R.C. v. Walgreen*
20 *Co.*, 733 F. Supp. 3d 876, 902 (C.D. Cal. 2024).

21 114. Defendant was not acting under the color of law to intercept Plaintiff's and Class
22 Members' wire or electronic communications.

23 115. Plaintiff and Class Members did not authorize Defendant to acquire the content of
24 their communications for purposes of invading Plaintiff's and Class Members' privacy. Plaintiff
25 and Class Members had a reasonable expectation that Defendant would not intercept their
26 communications and sell their data to dozens of parties without their knowledge or consent.

27 116. The foregoing acts and omission therefore constitute numerous violations of 18
28 U.S.C. § 2511(1), *et seq.*

117. As a result of each and every violation thereof, on behalf of herself and the Classes, Plaintiff seeks statutory damages of \$10,000 or \$100 per day for each violation of 18 U.S.C. § 2510, et seq. under 18 U.S.C. § 2520.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff seeks judgment against Defendant, individually and behalf of all others similarly situated, as follows:

- (a) For an order certifying the Class under Fed. R. Civ. P. 23, naming Plaintiff as the representative of the Class and Subclass, and naming Plaintiff's attorneys as class counsel to represent the Class and Subclass;
- (b) For equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;
- (c) For an order declaring that Defendant's conduct violates the statute referenced herein;
- (d) For an order finding in favor of Plaintiff and the Class on the count asserted herein;
- (e) For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and cost of suit;
- (f) For an award of damages, including, but not limited to, actual, consequential, statutory, punitive, and nominal damages, as allowed by law in an amount to be determined;
- (g) For prejudgment interest on all amounts awarded; and
- (h) Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

1 Dated: July 17, 2025

BURSOR & FISHER, P.A.

2 By: /s/ Julia K. Venditti
3 Julia K. Venditti

4 L. Timothy Fisher (State Bar No. 191626)
5 Julia K. Venditti (State Bar No. 332688)
6 Joshua R. Wilner (State Bar No. 353949)
7 1990 North California Blvd., 9th Floor
8 Walnut Creek, CA 94596
9 Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
jvenditti@bursor.com
jwilner@bursor.com

10 *Attorneys for Plaintiff and the Putative Class*