

1 Hal D. Cunningham (Bar No. 243048)
2 **SCOTT+SCOTT ATTORNEYS AT LAW**
3 **LLP**
4 600 W. Broadway, Suite 3300
5 San Diego, CA 92101
6 Telephone: (619) 223-4565
7 Facsimile: (619) 233-0508
8 hcunningham@scott-scott.com

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

[additional counsel listed on signature page]

7
8 **UNITED STATES DISTRICT COURT**
9 **NORTHERN DISTRICT OF CALIFORNIA**

10 JANE DOE, individually and on behalf of all
11 others similarly situated,
12
13 Plaintiff,
14
15 v.
16
17 GOOGLE LLC.
18
19 Defendant.

Case No.: _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

18 Plaintiff Jane Doe (“Plaintiff”), on behalf of herself and all others similarly situated, asserts
19 the following against Defendant Google LLC (“Google”) based upon personal knowledge, where
20 applicable, information and belief, and the investigation of counsel.

21 **SUMMARY OF ALLEGATIONS**

22 1. Google is one of the most valuable publicly traded companies in the world with a
23 market capitalization of over \$1 trillion dollars.

24 2. One of Google’s most lucrative businesses is its advertising and analytics services,
25 which alone generates hundreds of billions of dollars in advertising revenue for Google every year.

26 3. In connection with these services, Google makes a number of tracking tools,
27 including Google’s software development kits, tracking pixel, cookies, and other tracking
28 technology, including Google Analytics (collectively Google’s “Tracking Technology”), which are

1 used to collect data from the websites and mobile applications in which they are integrated.

2 4. Google's Tracking Technology is incorporated into third party websites through a
3 small piece of JavaScript code embedded on each page of the site. The code intercepts a user's
4 interactions, including any information they input and what they click, as they navigate each page
5 and sends that information, along with identifiable information, to Google for processing. Google
6 uses this data to provide marketing and analytics services as well as improve its ad targeting
7 capabilities and data points on users.

8 5. Alarminglly, Google's Tracking Technology is or was incorporated on the vast
9 majority of healthcare provider websites, including those of major institutions such as Planned
10 Parenthood, Keck Medicine of USC, MemorialCare: Long Beach Medical Center, and Sharp
11 HealthCare, and specifically on pages where patients can book appointments and access sensitive
12 health information.

13 6. For example, the Planned Parenthood website, www.plannedparenthood.org,
14 allows users to search for and schedule appointments for health care services (such as an abortion,
15 birth control, etc.) and prompts users to enter their zip code, city, or state, whether they are seeking
16 an in-person or telehealth appointment, and even at times to enter sensitive health information such
17 as the first day of their last period.

18 7. As users navigate the healthcare provider websites, Google's Tracking Technology
19 collects their sensitive information, including health information relating to sensitive medical
20 appointments, medical conditions, specific treatments, messages to healthcare providers, and
21 personally identifiable information ("PII").

22 8. Plaintiff used the Planned Parenthood website, which incorporated Google's
23 Tracking Technology, to search for an appointment for an abortion, selecting a facility in Burbank,
24 California.

25 9. Plaintiff, like other Class members, expected their private, personal sensitive
26 information (e.g., their searches, inputs, health information related to sensitive medical
27 appointments, medical conditions, specific treatments, messages to healthcare providers, and PII)

28

1 conveyed through healthcare provider websites to remain confidential.

2 10. However, unbeknownst to Plaintiff and Class members, Google intercepted and
3 collected their sensitive information, including their searches, inputs, health information relating to
4 private, personal, sensitive medical appointments, medical conditions, specific treatments, messages
5 to healthcare providers, and PII without consent.

6 11. Google's unlawful interception of Plaintiff's and Class members' communications
7 with healthcare provider websites constitutes an extreme invasion of privacy and violates federal
8 and state statutory and common law. Given the secret and undisclosed nature of Google's conduct,
9 additional evidence supporting Plaintiff's claims, including the full extent of how Google
10 intercepted Plaintiff's and Class members' private communications, and how they used that
11 information, will be revealed in discovery.

12 **PARTIES**

13 12. **Plaintiff Jane Doe** is a natural person and resident of Los Angeles County,
14 California.

15 13. Plaintiff used the Planned Parenthood website in 2018 to search for an abortion
16 provider through Planned Parenthood's scheduling pages.

17 14. Plaintiff clicked on a Planned Parenthood affiliate in Burbank, California on the
18 Planned Parenthood website.

19 15. Plaintiff then received treatment at this Planned Parenthood affiliate in Burbank,
20 California.

21 16. Plaintiff's private communications to Planned Parenthood, including her sensitive
22 information like being pregnant and searching for an abortion, were intercepted by Google through
23 Google's Tracking Technology incorporation on Planned Parenthood's website.

24 17. Plaintiff did not consent to Google's interception of her private, personal
25 information nor was Plaintiff provided notice of Google's interception and Plaintiff did not have the
26 opportunity to opt out of Google's interception.

27 18. Google used this information to, at least, provide marketing and analytics services
28

1 and to improve its software, algorithms, and other technology. Upon information and belief, this
2 information was also used by Google’s advertising offerings to create customer profiles, custom
3 audiences, and serve targeted advertisements.

4 19. **Defendant Google LLC** is a Delaware limited liability company with its principal
5 place of business located in Mountain View, California 94043.

6 20. Google, as the creator of its Tracking Technology and an established advertising
7 company, knew that it intercepted each of a user’s interactions on the website or mobile application
8 that incorporated this technology.

9 21. Accordingly, Google at all times knew that the incorporation of its Tracking
10 Technology into healthcare provider websites would result in its interception of sensitive
11 information, including health information relating to the scheduling of sensitive medical
12 appointments (for example, abortions), medical conditions, specific treatments, messages to
13 healthcare providers, and PII.

14 22. Indeed, this is not the first or last time Google has been called out for collecting
15 sensitive data like health information. For example, back in November 2019 the *Financial Times*
16 uncovered that Google received prescription drug names input by users on the website drugs.com.
17 In response to the report, Google claimed it had subsequently “marked” the data as sensitive
18 internally, excluding it from personalized ads, but that its technology may still serve “contextual”
19 ads from the content the user viewed.

20 23. Despite this, Google still took no action to prevent its Tracking Technology from
21 being embedded on healthcare provider websites from which it received sensitive health information
22 including their searches, inputs, health information relating to sensitive medical appointments,
23 medical conditions, specific treatments, messages to healthcare providers, and PII.

24 24. This is because Google does not want to stop collecting the data. Indeed, following
25 the Supreme Court’s decision in *Dobbs v. Jackson Women’s Health Organization*, several Google
26 employees requested an internal forum that “management . . . reconsider its data-sharing and
27 collection processes.” This request was ignored. Parul Koul, a Google software engineer, explained
28

1 that “users are concerned about, in light of this ruling, that Google will pass information on their
2 searches, communications, and location history to law enforcement and that this data will be used
3 to criminalize those seeking abortions.” He explained, “Google has completely failed to address this
4 concern.” Currently, Mr. Koul and the Alphabet Workers Union are “demand[ing] that Google
5 refuse to store any data that could be used to prosecute users in the U.S. [from] exercising their
6 bodily autonomy.”¹

7 25. As demonstrated by the incorporation of Google’s Tracking Technology on
8 healthcare provider websites, Google did not take any steps to prevent its interception and use of
9 users’ sensitive health data—including their searches, inputs, health information relating to sensitive
10 medical appointments, medical conditions, specific treatments, messages to healthcare providers,
11 and PII.

12 26. As such, Google’s conduct was intentional despite knowing the privacy violations it
13 caused to Plaintiff and Class members.

14 **JURISDICTION AND VENUE**

15 27. This Court has jurisdiction over the subject matter of this action pursuant to 28
16 U.S.C § 1332(d), because the amount in controversy for the Class exceeds \$5,000,000 exclusive of
17 interest and costs, there are more than 100 putative members of the Classes defined below, and a
18 significant portion of putative Class members are citizens of a state different from that of the
19 Defendant.

20 28. This Court has personal jurisdiction over Google because its principal place of
21 business is in California. Additionally, Google is subject to specific personal jurisdiction in this
22 State because a substantial part of the events and conduct giving rise to Plaintiff’s claims occurred
23 in this State, including Google’s collection of Plaintiff’s and Class members’ sensitive data from
24 healthcare provider websites and use of that data for commercial purposes.

25

26 ¹ Gerrit De Vynck, *Abortion is illegal for millions. Will Big Tech help prosecute it?*,
27 WASHINGTON POST (June 29 2022),
28 <https://www.washingtonpost.com/technology/2022/06/29/google-facebook-abortion-data/>

1 29. Venue is proper in this District pursuant to 28 U.S.C. §1391(b), (c), and (d) because
 2 a substantial portion of the conduct described in this Class Action Complaint was carried out in this
 3 District. Furthermore, Google is headquartered and resides in this District.

4 30. **Divisional Assignment:** This action arises in Santa Clara County, in that a
 5 substantial part of the events which give rise to the claims asserted herein occurred in Santa Clara
 6 County. Pursuant to L.R. 3-2(e), all civil actions that arise in Santa Clara County shall be assigned
 7 to the San Jose Division.

8 FACTUAL BACKGROUND

9 **I. Google's Tracking Technology**

10 31. Google is one of the most valuable publicly traded companies in the world with a
 11 market capitalization of over \$1 trillion dollars. Google fancies itself a “tech” company, but Google,
 12 at its core, is an advertising company.

13 32. Google “make[s] money” from “advertising products [that] deliver relevant ads at
 14 just the right time,” generating “revenues primarily by delivering both performance advertising and
 15 brand advertising.”² In 2020, Google generated \$146.9 billion in advertising revenue, which
 16 amounted to more than 80 percent of Google’s total revenues for the year. Google generated an even
 17 higher percentage of its total revenue from advertising in prior years:

18 Year	Total Revenue	Ad Revenue	% Ad Revenue
19 2021	\$257.6 billion	\$209.5 billion	81.33%
20 2020	\$182.5 billion	\$146.9 billion	80.49%
21 2019	\$161.9 billion	\$134.8 billion	83.29%
2018	\$136.8 billion	\$116.5 billion	85.12%

22 33. Google offers several analytics products, including its Tracking Technology, which
 23 exists solely to help drive ad revenue. For instance, Google Tracking Technology integrates with
 24 Google’s advertising offerings, such as Google Ads, Search Ads 360, Google Cloud, and Google
 25 Ad Manager, to direct more individuals to use Google’s ad network and products increasing
 26

27 ² ALPHABET INC., ANNUAL REPORT (FORM 10-K) (Feb. 2, 2021), available at
 28 <https://www.sec.gov/Archives/edgar/data/1652044/000165204421000010/goog-20201231.htm>.

1 Google’s overall ad revenue. Products like Google’s Tracking Technology also improve the
2 company’s advertising network and capabilities by providing more wholesome profiles and data
3 points on individuals.

4 34. Google first launched a version of Google Analytics in 2005 as a tool for website
5 traffic analysis. In 2007, Google launched Google Analytics Synchronous code with new tracking
6 functionality, such as the ability to track commerce transactions. Two years later, Google launched
7 the Google Analytics Asynchronous code, which allowed webpages to load faster and improved
8 data collection and accuracy.

9 35. Google continued updating its analytics platform, launching Universal Analytics in
10 2012. Universal Analytics offered new tracking codes and tools that provided more in-depth
11 information about user behavior. Also, Universal Analytics enabled tracking the same user across
12 multiple devices through its addition of the User-ID feature, which “associate[s] a persistent ID for
13 a single user with that user’s engagement data from one or more sessions initiated from one or more
14 devices.”

15 36. In 2020, Google launched Google Analytics 4, a platform combining Google
16 Analytics with Firebase to analyze both app and web activity.

17 37. Since launching Google Analytics, Google has become one of the most popular web
18 analytics platforms on the internet. Indeed, Google had a \$62.6 billion dollar increase in advertising
19 revenues in 2021, compared to 2020, after launching its most recent version of Google Analytics.

20 38. Google touts Google Analytics as a marketing platform that offers “a complete
21 understanding of your customers across devices and platforms.”³ It allows companies and
22 advertisers that utilize it to “understand how your customers interact across your sites and apps,
23 throughout their entire lifestyle,” “uncover new insights and anticipate future customer actions with
24 Google’s machine learning to get more value out of your data,” “take action to optimize marketing
25 performance with integrations across Google’s advertising and publisher tools,” and “quickly

26 _____
27 ³ *Analytics*, GOOGLE, <https://marketingplatform.google.com/about/analytics/> (last visited Jan.
28 10, 2023).

1 analyze your data and collaborate with an easy-to-use interface and shareable reports.”⁴

2 39. Google’s Tracking Technology is incorporated into third party websites by adding
3 a small piece of JavaScript measurement code to each page on the site. This code immediately
4 intercepts a user’s interaction with the webpage every time the user visits it, including what pages
5 they visit and what they click on. The code also collects identifiable information, such as the IP
6 address and Client ID.

7 40. Once Google’s Tracking Technology collects the data, it packages the information
8 and sends it to Google for processing in the Google Analytics platform. The Google Analytics
9 platform also allows the company or advertiser to customize the processing of the data, such as
10 applying filters. Once the data is processed, it is stored on a Google database and cannot be changed.

11 41. After the data has been processed and stored in the database, Google uses this data
12 to generate reports to help analyze the data from the webpages. These include reports on acquisition
13 (e.g., information about where your traffic originates, the methods by which users arrive at your site
14 or app, and the marketing efforts you use to drive traffic), engagement (e.g., measure user
15 engagement by the events and conversion events that users trigger and the web pages and app
16 screens that user visits), and demographics (e.g., classify your users by age, location, language, and
17 gender, along with interests they express through their online browsing and purchase activities).

18 42. In addition to using the data collected through its Tracking Technology to provide
19 marketing and analytics services, Google also uses the data to improve its ad targeting capabilities
20 and data points on users.

21 **II. Google’s Tracking Technology on Healthcare Provider Websites**

22 43. The implementation of Google’s Tracking Technology on healthcare provider
23 websites provides Google with a treasure trove of private, personal, highly sensitive and valuable
24 information regarding Plaintiff’s and Class members’ medical conditions, treatments, and
25 appointments.

26

27 ⁴ *Id.*

28

1 44. For example, through Google’s Tracking Technology incorporated on the Planned
2 Parenthood website, Google intercepted users’ interactions, including private, sensitive health
3 information such as whether the user is pregnant or scheduling an abortion. As a result, the
4 information Plaintiff provided, clicked, and searched for on the Planned Parenthood website to
5 locate an abortion provider was intercepted by Google in violation of state, federal, and common
6 law.

7 45. An investigation by *Lockdown Privacy* confirmed the same, revealing that Google
8 Tracking Technology intercepted private, personal information regarding the user’s interaction with
9 the Planned Parenthood website, including its scheduling pages. Google’s Tracking Technology
10 intercepts, at a minimum, the user’s IP address, the site visited, behavior on the site, reason for
11 visiting the site (e.g., “abortion”), the user’s selected method of abortion (e.g., surgical abortion/in-
12 clinic), the browser time zone, the name of the Planned Parenthood Health Center for the
13 appointment, the user’s approximate zip code, the user’s closest Planned Parenthood affiliate based
14 on their zip code, a time stamp, whether the user came from a search engine, a link, or typed the
15 URL directly, the user’s Client ID, and the browser language.

16 46. Other independent testing also reveals Google’s interception of users’ interactions
17 on the Planned Parenthood website. Using *The Markup*’s “Blacklight” tool confirms that Google’s
18 Tracking Technology is incorporated on Planned Parenthood’s scheduling pages. The Blacklight
19 tool works by visiting a website with a headless browser and running custom software in the
20 background of the webpage that monitors scripts and network connections. It then logs which scripts
21 call certain functions and generates a report. Specifically, the software was run by visiting Planned
22 Parenthood’s homepage, as well as its scheduling page to “Find a Health Center.”

23 47. The results showed Google’s Tracking Technology was incorporated on the “Find
24 a Health Center” page and “Abortion Clinics Near You” page and that, consequently, Google
25 received information about users’ activity on the page, including what they searched or sought
26 treatment for. Additionally, the results reveal that Google’s Tracking Technology likely had enabled
27 its “remarketing audiences,” which allows a user to be tracked across the internet. Lastly, Google’s
28

1 parent company, Alphabet, Inc., embedded third party cookies. Third party cookies are set by the
2 third party (here, Alphabet, Inc.) by embedding JavaScript into the website that allows the user to
3 be tracked across multiple websites.

4 48. But Planned Parenthood is not the only healthcare provider website that incorporates
5 Google's Tracking Technology. Indeed, the vast majority do, including major hospitals and medical
6 centers like Keck Medicine of USC, MemorialCare: Long Beach Medical Center, and Sharp
7 HealthCare, for example.

8 49. Analyzing these websites using the Blacklight tool has also confirmed Google's
9 interception of users' interactions through the incorporation of Google's Tracking Technology,
10 including on the appointment scheduling page of Keck Medicine of USC, MemorialCare: Long
11 Beach Medical Center, and patient portals, such as Sharp HealthCare. Plaintiff expects discovery to
12 reveal a complete list of websites using or that have used Google's Tracking Technology and the
13 data Google intercepted from those sites, which is information exclusively in its control.

14 50. Plaintiff and Class members did not consent to the interception of their data by
15 Google. Google's interception of Plaintiff's and Class members' private, personally sensitive
16 information, including their searches, inputs, health information relating to sensitive medical
17 appointments, medical conditions, specific treatments, messages to healthcare providers, and PII,
18 without their consent, is an invasion of privacy and violates several laws, including the California
19 Confidentiality of Medical Information Act ("CMIA") and the California Invasion of Privacy Act
20 ("CIPA").

21 **III. Plaintiff and Class Members Do Not Consent to Google's Interception of Their**
22 **Sensitive Information**

23 51. Plaintiff and Class members had no way of knowing Google intercepted their
24 sensitive information, including, for example, when searching for and scheduling appointments
25 through healthcare providers' scheduling pages, and when using patient portals to schedule
26 appointments, access information about their medical treatments, and contact their medical provider,
27 because Google's software is seamlessly incorporated in the background.
28

1 52. Thus, Plaintiff and all Class members could not consent to Google’s conduct when
2 they were unaware their confidential communications would be intercepted, stored, and used in the
3 first place.

4 **IV. Plaintiff and Class Members Have a Reasonable Expectation of Privacy in Their**
5 **User Data**

6 53. Plaintiff and Class members have a reasonable expectation of privacy in their
7 confidential communications, including information relating to their searches for and scheduling of
8 abortions and other medical services, and their sensitive medical information.

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

12 55. For example, a recent study by *Consumer Reports* shows that 92% of Americans
13 believe that websites should be required to provide consumers with a complete list of the data that
14 has been collected about them. Moreover, according to a study by *Pew Research Center*, a majority
15 of Americans, approximately 79%, are concerned about how data is collected about them by
16 companies.

17 56. Users act consistent with these preferences. Following a new rollout of the iPhone
18 operating software—which asks users for clear, affirmative consent before allowing companies to
19 track users—85% of worldwide users and 94% of U.S. users chose not to share data when prompted.
20 Another recent study by *DataGrail* revealed that 67% of people were willing to pay \$100 or more
21 annually to keep their information out of the hands of companies and the government. The same
22 study revealed that 75% of people would abandon brands that do not take care of their data.

23 57. The expectation of privacy in this specific type of data is especially heightened in
24 light of the recent Supreme Court decision in *Dobbs v. Jackson Women’s Health Organization*,
25 overturning the constitutional right to abortion, with many states banning abortion all together.
26 Indeed, 66% of younger women are making privacy-related changes, deleting, or are planning to
27 delete period tracker apps on their devices as *Roe v. Wade* is now overturned. Google’s conduct is
28

1 particularly intrusive and offensive in light of this decision, as this type of highly sensitive
2 information can potentially be turned over in response to a criminal subpoena.

3 58. Google’s surreptitious interception, storage, and use Plaintiff’s and Class members’
4 sensitive information, including health information relating to sensitive medical appointments,
5 medical conditions, and medical treatments violates Plaintiff’s and Class members’ privacy
6 interests.

7 **V. The Data Google Intercepted is Plaintiff’s Property, Has Economic Value, and its**
8 **Interception Caused Economic Harm**

9 59. It is common knowledge in the industry that there is an economic market for
10 consumers’ personal data—including the data Google intercepted from Plaintiff and Class members.

11 60. In 2013, the *Financial Times* reported that the data-broker industry profits from the
12 trade of thousands of details about individuals, and that within that context, age, gender, and location
13 information sold for \$.50 per 1,000 people. This estimate was based upon industry pricing data
14 viewed by the *Financial Times* at the time.

15 61. In 2015, *TechCrunch* reported that to obtain names of individuals who have
16 particular diseases, a market participant would need to spend \$.30 per name. That same article
17 explained that a single user’s data can vary from \$15 to \$40.

18 62. Notably, a 2021 report from *Invisibly* found that personal medical information is
19 one of the *most valuable pieces of data* within this data-market. “It’s worth acknowledging that
20 because health care records often feature a more complete collection of the patient’s identity,
21 background, and personal identifying information (PII), health care records have proven to be of
22 particular value to criminals.”⁵ “While a single social security number might go for \$0.53, a
23 complete health care record sells for \$250 on average. For criminals, the more complete a dataset,
24 the more potential value they can get out of it. As a result, health care breaches increased by 55%

25
26
27 ⁵ *How Much is Your Data Worth? The Complete Breakdown for 2021*, INVISIBLY, (July 13,
28 2021), <https://www.invisibly.com/learn-blog/how-much-is-data-worth/>.

1 in 2020.”⁶ 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

13 63. The Federal Trade Commission has also confirmed the value of user data and,
14 particularly, health information. It found back in 2014 that data brokers sell data that categorize
15 users into sensitive categories, such as “expectant parent.”⁷ It recently sued one of these companies
16 for selling location data on people who visit abortion clinics for approximately \$160 for a week’s
17 worth of data. Experian also refers to health data as a “gold mine” for healthcare companies and
18 clinicians.

19 64. For instance, Datarade.ai advertises access to U.S. customers names, addresses,
20 email addresses, and the telephone numbers of people who bought brand name medicine. Even only
21 some of this data may sell for \$10,000. Other companies, like Pfizer, spend \$12 million annually to
22 purchase health data. This is not surprising given that the medical data industry was valued at over
23 \$2.6 billion back in 2014.

24 _____
25 ⁶ *Id.*

26 ⁷ DATA BROKERS, A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, FEDERAL TRADE
27 COMMISSION, (May 2014), available at <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.
28

1 individual actions alleging the same claims.

2 71. **Numerosity:** All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The
3 members of the Classes are so numerous and geographically dispersed that individual joinder of all
4 Class members is impracticable. While Plaintiff is informed and believes that there are likely tens
5 of thousands, if not millions, of members of the Classes, the precise number of Class members is
6 unknown to Plaintiff. Class members may be identified through objective means, including
7 Defendant's own records. Class members may be notified of the pendency of this action by
8 recognized, court-approved notice dissemination methods, which may include U.S. mail, electronic
9 mail, internet postings, and/or published notice.

10 72. **Commonality and Predominance:** All requirements of Fed. R. Civ. P. 23(a)(2)
11 and 23(b)(3) are satisfied. This action involves common questions of law and fact, which
12 predominate over any questions affecting individual Class members, including, without limitation:

- 13 a. Whether Google's acts and practices violated the California Invasion of Privacy Act, Cal.
14 Penal Code §§ 630, *et seq.*;
- 15 b. Whether Google's acts and practices violated Plaintiff's and Class members' privacy rights;
- 16 c. Whether Google's acts and practices violated California Constitution, Art. 1, § 1;
- 17 d. Whether Google's acts and practices violated California's Confidentiality of Medical
18 Information Act, Civil Code §§ 56, *et seq.*;
- 19 e. Whether Google was unjustly enriched;
- 20 f. Whether Plaintiff and the Class members are entitled to equitable relief, including but not
21 limited to, injunctive relief, restitution, and disgorgement; and
- 22 g. Whether Plaintiff and the Class members are entitled to actual, statutory, punitive or other
23 forms of damages, and other monetary relief.

24 73. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the
25 Classes. The claims of Plaintiff and the members of the Classes arise from the same conduct by
26 Defendant and is based on the same legal theories.

27 74. **Adequate Representation:** Plaintiff has and will continue to fairly and adequately
28 represent and protect the interests of the Classes. Plaintiff has retained counsel competent and

1 experienced in complex litigation and class actions, including litigations to remedy privacy
2 violations. Plaintiff has no interest that is antagonistic to the interests of the Classes, and Defendant
3 has no defenses unique to any Plaintiff. Plaintiff and her counsel are committed to vigorously
4 prosecuting this action on behalf of the members of the Classes, and they have the resources to do
5 so. Neither Plaintiff nor her counsel have any interest adverse to the interests of the other members
6 of the Classes.

7 75. **Substantial Benefits:** This class action is appropriate for certification because class
8 proceedings are superior to other available methods for the fair and efficient adjudication of this
9 controversy and joinder of all members of the Classes is impracticable. This proposed class action
10 presents fewer management difficulties than individual litigation, and provides the benefits of single
11 adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment
12 will create economies of time, effort, and expense and promote uniform decision-making. Plaintiff
13 reserves the right to revise the foregoing class allegations and definitions based on facts learned and
14 legal developments following additional investigation, discovery, or otherwise.

15 **CALIFORNIA LAW APPLIES TO BOTH CLASSES**

16 76. California substantive laws apply to every member of the Classes. California's
17 substantive laws may be constitutionally applied to the claims of Plaintiff and the Classes under the
18 Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the U.S.
19 Constitution. California has significant contact, or significant aggregation of contacts, to the claims
20 asserted by Plaintiff and Class members, thereby creating state interests to ensure that the choice of
21 California state law is not arbitrary or unfair.

22 77. Google maintains its principal places of business in California and conducts
23 substantial business in California, such that California has an interest in regulating Google's conduct
24 under its laws. Google also selected California law as the law to govern all disputes with its
25 customers in its Terms of Service. Google's decision to reside in California and avail itself of
26 California's laws, renders the application of California law to the claims herein constitutionally
27 permissible.

1 healthcare provider websites expressly represented this information would remain anonymous and
2 confidential.

3 86. Plaintiff and Class members were not aware that Google intercepted their data,
4 including their sensitive information.

5 87. Plaintiff and Class members exercised due diligence to uncover the facts alleged
6 herein and did not have actual or constructive knowledge of Google’s misconduct by virtue of their
7 fraudulent concealment.

8 88. Accordingly, all statutes of limitations are tolled under the doctrine of fraudulent
9 concealment.

10 **CLAIMS FOR RELIEF**

11 **FIRST CLAIM FOR RELIEF**

12 **Violation of Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class and Subclass)**

13 89. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint
14 with the same force and effect as if fully restated herein.

15 90. A Plaintiff asserting claims for intrusion upon seclusion must plead (1) that the
16 defendant intentionally intruded into a matter as to which the plaintiff has a reasonable expectation
17 of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

18 91. Google’s surreptitious interception, storage, and use of Plaintiff’s and Class
19 members’ interactions and communications with healthcare provider websites, such as Planned
20 Parenthood’s website, including health information pertaining to a user’s reproductive health and
21 seeking of medical treatment, constitutes an intentional intrusion upon Plaintiff’s and Class
22 members’ solitude or seclusion.

23 92. Plaintiff and Class members had a reasonable expectation of privacy in this
24 information. Plaintiff’s private communications with the healthcare providers through their websites
25 and patient portals are inherently sensitive in nature, especially those relating to booking
26 appointments. Plaintiff and Class members reasonably expected this information would remain
27 private and confidential and would not be intercepted by a third party without their consent.

28

1 93. Plaintiff and Class members did not consent to, authorize, or know about Google’s
2 intrusion at the time it occurred. Plaintiff and Class members never agreed that Google could
3 intercept their user data, including sensitive information.

4 94. The surreptitious taking and interception of sensitive user data from thousands, if
5 not millions of individuals, was highly offensive (and would be to a reasonable person) because it
6 violated expectations of privacy that have been established by social norms. Privacy polls and
7 studies show that the overwhelming majority of Americans believe one of the most important
8 privacy rights is the need for an individual’s affirmative consent before personal data is collected or
9 shared.

10 95. The offensiveness of this conduct is all the more apparent because Google’s
11 interception, storage, and use of this sensitive information was conducted inconspicuously in a
12 manner that Plaintiff and Class members would be unable to detect. As a result of Google’s actions,
13 Plaintiff and Class members have suffered harm and injury, including but not limited to an invasion
14 of their privacy rights.

15 96. Plaintiff and Class members have been damaged as a direct and proximate result of
16 Google’s invasion of their privacy and are entitled to just compensation, including monetary
17 damages.

18 97. Plaintiff and Class members seek appropriate relief for that injury, including but not
19 limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to
20 their privacy interests as well as a disgorgement of profits made by Google as a result of its intrusions
21 upon Plaintiff’s and Class members’ privacy.

22 98. Plaintiff and Class members are also entitled to punitive damages resulting from the
23 malicious, willful, and intentional nature of Google’s actions, directed at injuring Plaintiff and Class
24 members in conscious disregard of their rights. Such damages are needed to deter Google from
25 engaging in such conduct in the future.

26 Plaintiff also seeks such other relief as the Court may deem just and proper.
27
28

SECOND CLAIM FOR RELIEF

**Violation of the California Constitution, Art. 1, § 1 – Invasion of Privacy
(On Behalf of Plaintiff and the Subclass)**

1
2
3 99. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint
4 with the same force and effect as if fully restated herein.

5 100. Art. I, § 1 of the California Constitution provides: “All people are by nature free
6 and independent and have inalienable rights. Among these are enjoying and defending life and
7 liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety,
8 happiness, and privacy.”

9 101. The right to privacy in the California Constitution creates a private right of action
10 against private and government entities. To state a claim for invasion of privacy under the California
11 Constitution, a Plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable
12 expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact
13 as to constitute an egregious breach of the social norms.

14 102. Plaintiff and Class members have a legally protected privacy interest in their private
15 communications with healthcare provider websites, such as Planned Parenthood’s website,
16 including information relating to their identities, pursuant to Art. I, § 1 of the California Constitution.
17 Plaintiff’s and Class members’ private communications with the healthcare providers through the
18 healthcare provider websites are inherently sensitive in nature, especially those relating to booking
19 appointments.

20 103. Plaintiff and Class members had a reasonable expectation of privacy under the
21 circumstances, including that: (i) the private communications intercepted by Google include
22 personal, sensitive information related to their health and Plaintiff’s and Class members’ identities;
23 and (ii) Plaintiff and Class members did not consent or otherwise authorize Google to intercept,
24 store, or use this private information for its own monetary gain.

25 104. The private communications, which Google intruded upon and intercepted without
26 Plaintiff’s and Class members’ authorization or consent, included extremely sensitive information
27 like whether a user was pregnant and scheduled an abortion. Google’s actions constituted an
28

1 egregious breach of the social norms, including because: (i) the data intercepted was highly sensitive
2 and personal, as protected by the California Constitution; (ii) Google did not have authorization or
3 consent to collect this information; and (iii) the invasion deprived Plaintiff and Class members the
4 ability to control the circulation of said information, which is considered a fundamental right to
5 privacy.

6 105. Plaintiff and Class members have sustained damages and will continue to suffer
7 damages as a direct and proximate result of Google’s conduct, including an invasion of privacy.

8 106. Plaintiff and Class members seek appropriate relief for that injury, including but not
9 limited to damages that will reasonably compensate Plaintiff and Class members for the harm to
10 their privacy interests as well as a disgorgement of profits made by Google as a result of its intrusions
11 upon Plaintiff’s and Class members’ privacy.

12 107. Plaintiff and Class members are also entitled to punitive damages resulting from the
13 malicious, willful, and intentional nature of Google’s actions, directed at injuring Plaintiff and Class
14 members in conscious disregard of their rights. Such damages are needed to deter Google from
15 engaging in such conduct in the future.

16 108. Plaintiff also seeks such other relief as the Court may deem just and proper.

17 **THRID CLAIM FOR RELIEF**
18 **Violation of the California Invasion of Privacy Act (“CIPA”)**
19 **(Cal. Penal Code § 631 *et seq.*)**
20 **(On Behalf of the Plaintiff and Class and Subclass)**

21 109. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint
22 with the same force and effect as if fully restated herein.

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

1 protect the right of privacy of the people of this state.” *Id.*

2 111. Cal. Penal Code § 631 imposes liability on any person who “by means of any
3 machine, instrument, or contrivance, or in any other manner” (1) “intentionally taps, or makes any
4 unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument,” (2)
5 “willfully and without the consent of all parties to the communication, or in any unauthorized
6 manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or
7 communication while the same is in transit or passing over any wire, line, or cable, or is being sent
8 from, or received at any place within [the state of California],” (3) “uses, or attempts to use, in any
9 manner, or for any purpose, or to communicate in any way, any information so obtained,” or (4)
10 “aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or
11 cause to be done any of the acts or things mentioned above in this section.”

12 112. Google is a person for purposes of § 631.

13 113. Google maintains its principal places of business in California, where it designed,
14 contrived, agreed, conspired, effectuated, and/or received the interception and use of the contents of
15 Plaintiff’s and Class members’ sensitive communications. Additionally, Google has adopted
16 California substantive law to govern its relationship with users. Google intercepted Plaintiff’s
17 confidential communications in California where she is located.

18 114. Google’s Tracking Technology, Plaintiff’s and Class members’ browsers, and
19 Plaintiff’s and Class members’ computing and mobile devices are a “machine, instrument, or
20 contrivance, or . . . other manner.”

21 115. At all relevant times, Google, using Google’s Tracking Technology, intentionally
22 tapped or made unauthorized connections with the lines of internet communication between Plaintiff
23 and Class members and the healthcare providers without the consent of all parties to the
24 communication.

25 116. Google, willfully and without the consent of Plaintiff and Class members, read or
26 attempted to read, or learned the contents or meaning of Plaintiff’s and Class members’ sensitive
27 communications to the healthcare providers while the communications were in transit or passing
28

1 over any wire, line or cable, or were being received at any place within California when it intercepted
2 Plaintiff's and Class members' sensitive communications and data with the healthcare providers in
3 real time.

4 117. Google used or attempted to use the communications and information it received
5 through Google's Tracking Technology, including to supply its analytics and advertising services
6 and improve its technology.

7 118. The interception of Plaintiff's and Class members' sensitive communications was
8 without authorization and consent from the Plaintiff and Class members. Accordingly, the
9 interception was unlawful and tortious.

10 119. Plaintiff and the Class members seek statutory damages in accordance with
11 § 637.2(a), which provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount
12 of damages sustained by Plaintiff and the Class in an amount to be proven at trial, as well as
13 injunctive or other equitable relief.

14 120. Plaintiff and Class members have also suffered irreparable injury from these
15 unauthorized acts. Plaintiff's and Class members' sensitive data has been collected, viewed,
16 accessed, stored, by Google, has not been destroyed, and due to the continuing threat of such injury,
17 Plaintiff and Class members have no adequate remedy at law. Plaintiff and Class members are
18 entitled to injunctive relief.

19 **FOURTH CLAIM FOR RELIEF**
20 **Violation of CIPA**
21 **Cal. Penal Code § 632**
22 **(On Behalf of Plaintiff and Class and Subclass)**

23 121. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint
24 with the same force and effect as if fully restated herein.

25 122. Cal. Penal Code § 632 prohibits "intentionally and without the consent of all parties
26 to a confidential communication," the "use[] [of] an electronic amplifying or recording device to
27 eavesdrop upon or record the confidential communication."
28

1 123. § 632 defines “confidential communication” as “any communication carried on in
2 circumstances as may reasonably indicate that any party to the communication desires it to be
3 confined to the parties thereto[.]”

4 124. Plaintiff’s and Class members’ communications to healthcare and medical providers
5 through healthcare and medical provider websites, including their sensitive information such as
6 information concerning reproductive health services and other medical information were
7 confidential communications for purposes of § 632, including because Plaintiff and Class Members
8 had an objectively reasonable expectation of privacy in this data.

9 125. Plaintiff and Class members expected their communications to the healthcare
10 providers through healthcare provider websites would not be intercepted by Google. Plaintiff and
11 Class members did not expect Google to secretly eavesdrop upon or record this information and
12 their communications.

13 126. Google’s Tracking Technology is an electronic amplifying or recording device for
14 purposes of § 632.

15 127. By contemporaneously intercepting and recording Plaintiff’s and Class members’
16 confidential communications to the healthcare providers through Google’s Tracking Technology,
17 Google eavesdropped and/or recorded confidential communications through an electronic
18 amplifying or recording device in violation of § 632 of CIPA.

19 128. At no time did Plaintiff or Class members consent to Google’s conduct, nor could
20 they reasonably expect that their communications to the healthcare providers through the healthcare
21 provider websites, would be overheard or recorded by Google.

22 129. Google utilized Plaintiff’s and Class members’ sensitive personal information for
23 their own purposes, including advertising and analytics.

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

28

1 131. Plaintiff and Class members have also suffered irreparable injury from these
2 unauthorized acts. Plaintiff's and Class members' sensitive data has been collected, viewed,
3 accessed, stored, by Google, has not been destroyed, and due to the continuing threat of such injury,
4 have no adequate remedy at law. Plaintiff and Class members are entitled to injunctive relief.

5 **FIFTH CLAIM FOR RELIEF**
6 **Violation of CMIA**
7 **Cal. Civ. Code § 56.36**
8 **(On Behalf of Plaintiff and Class and Subclass)**

9 132. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint
10 with the same force and effect as if fully restated herein.

11 133. Cal. Civ. Code § 56.36(B)(3)(A) prohibits any person of entity other than a licensed
12 healthcare professional from knowingly or willfully obtaining medical information for financial
13 gain.

14 134. Cal. Civ. Code § 56.36(B)(5) prohibits any person or entity who is not permitted to
15 receive medical information under the CMIA from knowingly and willfully obtaining, disclosing,
16 or using the medical information without written authorization.

17 135. The CMIA defines "medical information" to mean any "individually identifiable
18 information" in possession of or derived from "a provider of health care, health care service plan,
19 pharmaceutical company, or contractor regarding a patient's medical history, mental or physical
20 condition, or treatment." The information the healthcare providers maintained and disclosed is
21 medical information because it is identifiable information relating to a patient's medical condition,
22 reproductive health, and subsequent plan of treatment.

23 136. Accordingly, the healthcare providers are providers of health care under Cal. Civ.
24 Code § 56.06, subdivisions (a) and (b), because the healthcare providers maintain medical
25 information and offer software to consumers that is designed to maintain medical information for
26 the purposes of allowing their users to manage their information or make the information available
27 to a healthcare provider, or for the diagnoses, treatment, or management of a medical condition.
28

1 137. The CMIA defines “patient” to mean any natural person, whether or not still living,
2 who received health care services from a provider of health care and to whom medical information
3 pertains. Plaintiff is a living person who received health care services from a provider of health
4 care, under § 56.06, and the medical information pertains to her specifically.

5 138. Google is an entity who is not a licensed health care professional and is not permitted
6 to receive medical information under the CMIA.

7 139. Google violated Cal. Civ. Code § 56.36(B)(3)(A) and (B)(5) because it knowingly
8 and willfully obtained medical information from the healthcare provider websites without
9 authorization for its own financial gain.

10 140. As described herein, Google intentionally designed Google’s Tracking Technology
11 to intercept data from the websites in which they are incorporated.

12 141. Google knew Google’s Tracking Technology was incorporated on the healthcare
13 provider websites, including Planned Parenthood’s website, and that it would consequently lead to
14 the interception of medical information maintained by the healthcare providers.

15 142. Google knowingly and willfully received this information without written
16 authorization from Plaintiff and Class members, and did so for its own financial gain. Namely, to
17 profit through advertising and analytics services it offers, as well as to improve its algorithms, data
18 points, and other technologies.

19 143. Pursuant to Cal. Civ. Code § 56.36(B)(3)(A) and Cal. Civ. Code § 56.36(B)(5),
20 Google is liable for a civil penalty up to \$250,000 per violation of these sections.

21 **SIXTH CLAIM FOR RELIEF**
22 **Aiding and Abetting Violation of CMIA**
23 **Cal. Civ. Code §§ 56.06, 56.101, 56.10**
24 **(On Behalf of Plaintiff and Class and Subclass)**

25 144. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint
26 with the same force and effect as if fully restated herein.

27 145. Although not parties to this action, the healthcare providers disclosed Plaintiff’s and
28 Class members’ medical information, which violated §§ 56.06, 56.101, and 56.10 of CMIA. Google

1 is therefore subject to the same violations because it aided and abetted the healthcare providers in
2 violating these sections.

3 146. The healthcare providers violated Cal. Civ. Code § 56.06(e) because they did not
4 maintain the confidentiality of users' medical information. The healthcare providers disclosed to
5 Google, a third party, Plaintiff's and Class members' medical information without consent.

6 147. The healthcare providers violated Cal. Civ. Code § 56.101, subdivision (a), because
7 they failed to maintain, preserve, and store medical information in a manner that preserves the
8 confidentiality of the information contained therein because they disclosed to Google Plaintiff's and
9 Class members' medical information.

10 148. The healthcare providers violated Cal. Civ. Code § 56.10, subdivision (a), because
11 they disclosed medical information without first obtaining authorization when they disclosed to
12 Google Plaintiff's and Class members' data, including medical information.

13 149. By contracting with the healthcare providers to receive and use Plaintiff's and Class
14 members' data and communications, including medical information, as well as providing the means
15 to accomplish this objective, Google acted intentionally, or alternatively, with knowledge that the
16 healthcare providers' misappropriation of Plaintiff's and Class members' medical information was
17 a violation of the CMIA.

18 150. Google provided substantial assistance and encouragement to healthcare providers'
19 violation of the CMIA, including by providing the means, i.e., Google's Tracking Technology, to
20 share and disclose this data. Google knew that its software could be seamlessly integrated without
21 alerting users that their sensitive medical information would be shared with Google.

22 151. Google's agreements with the healthcare providers and receipt of Plaintiff's and
23 Class members' sensitive information, including medical information, are a substantial factor in
24 causing the violations of the CMIA alleged herein. For example, in the absence of Google's
25 software, the healthcare providers would likely not have shared Plaintiff's and Class members'
26 medical information with Google.

27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

SCOTT+SCOTT ATTORNEYS AT LAW LLP
Joseph P. Guglielmo (*pro hac vice* forthcoming)
Carey Alexander (*pro hac vice* forthcoming)
230 Park Ave., 17th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com
calexander@scott-scott.com

SCOTT+SCOTT ATTORNEYS AT LAW LLP
Erin Green Comite (*pro hac vice* forthcoming)
156 South Main Street
P.O. Box 192
Colchester, CT 06415
Telephone: (860) 537-5537
ecomite@scott-scott.com

Attorneys for Plaintiff and the Proposed Class

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Google Facing Class Action Over Alleged Data Tracking on Healthcare Provider Websites](#)
