

**IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA**

**CONNIE HOWARD, YADIRA YAZMIN)
HERNANDEZ, and DEBORAH)
REYNOLDS, on behalf of themselves and)
all others similarly situated,)**

Civil Action No. 1:23-cv-00758-UA-JEP

Plaintiffs,)

**AMENDED CLASS ACTION
COMPLAINT**

v.)

**LABORATORY CORPORATION OF)
AMERICA, and LABORATORY)
CORPORATION OF AMERICA)
HOLDINGS.)**

Defendants.

Plaintiffs Connie Howard, Yadira Yazmin Hernandez, and Deborah Reynolds (“Plaintiffs”), individually and on behalf of California and Pennsylvania Classes of all other similarly situated persons, bring this action against Laboratory Corporation of America and Laboratory Corporation of America Holdings (collectively, “Labcorp” or “Defendants”) for violating California’s and Pennsylvania’s wiretapping laws: the California Invasion of Privacy Act, Cal. Penal Code § 631 (“CIPA”) and the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. § 5703 (“WESCA”).

NATURE OF THE CASE

1. This is a class action against Labcorp for knowingly enabling third parties like Meta and Google to obtain individually identifiable information alongside the contents of confidential electronic communications from Plaintiffs, in a manner that violates California and Pennsylvania law.

2. Labcorp knowingly employs and configured hidden tracking code on its website, labcorp.com, to surreptitiously track the activities of people using Labcorp’s homepage to search for sensitive medical information. The code Labcorp chose to place and configure on its website is created by Meta Platforms, Inc. (formerly known as Facebook) (“Meta”), Google LLC (“Google”), and others (collectively, “Third-party Trackers”). Labcorp’s decision to install these Third-party Trackers and the way it chose to configure them has facilitated the disclosure of large quantities of sensitive data on a daily basis from Labcorp’s website to the Third-Party Trackers.

3. As described more fully below, this sensitive data and information includes the identities of persons who visited Labcorp’s website, the specific search terms they entered into the website’s search bar (e.g., searches concerning medical conditions and tests), the pages they visited on the Labcorp website resulting from those sensitive searches, and specific medical tests

and related codes generated by the same searches Class members' affirmatively indicated an interest in. Upon information and belief, the Third Party Trackers combined this sensitive information with information about each user gathered from other sources and used it for purposes not authorized by the persons from whom the data was taken. Labcorp website users were not advised that third parties collect this sensitive information, and Labcorp did not have Plaintiffs' or Class members' consent to disclose this information to third parties. California and Pennsylvania law expressly prohibit Labcorp's conduct.

4. The California Invasion of Privacy Act prohibits third parties like Meta and Google from learning the contents of Plaintiffs' and Class members' electronic communications to and from Labcorp without the consent of both the sender and recipient of the electronic communication, which the relevant third parties lacked, including the content of the communications described herein. CIPA also prohibits Labcorp from aiding, employing, or conspiring with third parties to engage in those unlawful activities, as alleged herein.

5. Pennsylvania's Wiretapping and Electronic Surveillance Control Act prohibits third parties from intercepting the contents of Plaintiffs' and Class members' electronic communications to and from Labcorp without the consent of both the sender and recipient of the electronic communication, which these third parties lacked, including the content of the communications described herein. WESCA also prohibits Labcorp from procuring third parties to engage in those unlawful activities.

6. Pursuant to Cal. Penal Code § 637.2 and 18 Pa. Cons. Stat. § 5725(a), Plaintiffs seek, on behalf of themselves and each member of the proposed California and Pennsylvania Classes, damages in an amount no less than all available statutory damages, injunctive relief, and such other equitable relief as the court determines appropriate.

PARTIES

7. Plaintiff Connie Howard (“Plaintiff Howard”) is a resident of Los Angeles, California.

8. Plaintiff Yadira Yazmin Hernandez (“Plaintiff Hernandez”) is a resident of San Diego, California.

9. Plaintiff Deborah Reynolds (“Plaintiff Reynolds”) is a resident of Hallam, Pennsylvania.

10. Defendant Labcorp is a Delaware Corporation with its headquarters in Burlington, North Carolina. Labcorp’s offices are located at 531 South Spring Street, Burlington, North Carolina, 27215.

11. Defendant Labcorp Holdings is a Delaware Corporation with its headquarters in Burlington, North Carolina. Labcorp’s offices are located at 358 South Main Street, Burlington, North Carolina, 27215.

JURISDICTION AND VENUE

12. This Court has personal jurisdiction over Labcorp because Labcorp has sufficient minimum contacts with this District in that it operates and markets its services throughout the country and in this District. Labcorp is also headquartered and has its principal place of business in this District.

13. This Court’s exercise of personal jurisdiction over Labcorp is also appropriate because Labcorp’s activities in North Carolina gave rise to and furthered the privacy violations suffered by Plaintiffs. Labcorp employed and configured the Third-party Trackers’ software code to intercept, record, and store data from and about visitors to its website conducting sensitive medical searches, for analysis and monetization by the Third-Party Trackers.

14. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d)(2) because

this is a class action with more than \$5,000,000 in controversy where at least one Class member is a citizen of a state of which one Defendant is not a citizen. Website performance data indicates that, between February 2023 and August 2023, there were over 30 million visits to the Labcorp website and a little over 5 million unique visits per month. Plaintiffs' good faith estimate based upon the populations of California and Pennsylvania indicate that there are at least many thousands of members in both the California and Pennsylvania Classes, resulting in damages that far exceeding \$5,000,000, exclusive of interest and costs.

15. Venue is appropriate in this Court because Labcorp resides in this District.

COMMON FACTUAL ALLEGATIONS

I. Background of CIPA

16. CIPA is a California state privacy law, which the California legislature enacted in 1967 to "protect the right of privacy of the people of this state" by, among other things, ensuring that communications would not be intercepted or recorded without consent from every party thereto. Cal. Penal Code § 630.

17. CIPA prohibits "[a]ny person" from "willfully and without the consent of all parties to the communication...read[ing], or attempt[ing] to read, or to 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 who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained." Cal. Penal Code § 631.

18. CIPA furthermore prohibits "aid[ing], agree[ing] with, employ[ing], or conspire[ing] with any person or persons to unlawfully do, or permit, or cause to be done" any of the conduct at issue. *Id.*

II. Background on WESCA

19. WESCA is the Pennsylvania state wiretap law, which the Pennsylvania legislature most recently amended in 1988.

20. WESCA prohibits “a person” from “(1) intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept any wire, electronic or oral communication; (2) intentionally disclos[ing] or endeavor[ing] to disclose to any other person the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication; or (3) intentionally us[ing] or endeavor[ing] to use the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know, that the information was obtained through the interception of a wire, electronic or oral communication.” 18 Pa. Cons. Stat. § 5703.

III. Background on Third-party Trackers’ Software Code Implemented By Labcorp

21. The Third-party Trackers create snippets of computer code that companies like Labcorp can choose to incorporate and embed in their websites to collect and send information about their users’ interaction with those websites to third parties, often for advertising purposes.¹ As described more fully below, Labcorp not only affirmatively chose to place the Third-Party Trackers’ code on its website’s homepage, but also decided what website user data the Third-Party Trackers should intercept, and specifically configured them to collect and disclose that same information to Meta, Google, and others.² Labcorp has used two of the most widely

¹ CookiePro, *What is a Tracking Pixel?* (Sept. 17, 2021), <https://www.cookiepro.com/knowledge/tracking-pixel/> [https://perma.cc/8Y8U-48K7]; James Milin-Ashmore, Comparitech, *What is a Tracking Pixel?* (February 26, 2023), <https://www.comparitech.com/blog/information-security/what-is-a-tracking-pixel/> [https://perma.cc/AD9C-MH3C].

² Meta, *How to set up and install a Meta Pixel*,

implemented tracking codes to engage in this illegal conduct: the Meta Pixel and Google Analytics.³

B. The Meta Pixel

22. Meta is an advertising company that sells advertising space on the social media platforms it operates. Meta's advertising is based on sophisticated user-categorizing and targeting capabilities that are fueled by the personal data of users of the social media platforms and other Internet users.⁴ Meta's targeting abilities are exceptional because Meta surveils users' online activities, both on and off Meta's own websites and apps.⁵ This expansive tracking enables Meta to make highly personal inferences about users, such as about their "interests," "behavior," and "demographics."⁶ Meta compiles information it obtains, makes such inferences, and then uses them to identify personalized "audiences" likely to respond to particular advertisers' messaging. Access to such audiences is extremely valuable to Meta's advertising clients. In 2022, Meta generated approximately \$113.64 billion, nearly 98% of its revenue, through advertising.

<https://www.facebook.com/business/help/952192354843755?id=1205376682832142> [<https://perma.cc/74X5-QVGJ>] (describing the process for setting up and installing a Meta Pixel); Google, *[GA4] Set up Analytics for a website and/or app*, <https://support.google.com/analytics/answer/9304153?hl=en> [<https://perma.cc/U3S7-844F>] (describing the process for setting up and installing Google Analytics code).

³ Usman Qureshi, MeasureSchool, *Meta Pixel vs Google Analytics 4* (Feb. 15, 2023), <https://measureschool.com/meta-pixel-vs-google-analytics-4/> [<https://perma.cc/GPQ5-TQAC>].

⁴ Meta Business Help Center, *Why advertise on Facebook, Instagram and other Meta technologies*, <https://www.facebook.com/business/help/205029060038706> [<https://perma.cc/NES6-5W8D>].

⁵ Meta Business Help Center, *About Meta Pixel*, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142> [<https://perma.cc/VWK8-7MCH>]; Meta, *Facebook Core Audience Targeting*, <https://www.facebook.com/business/news/Core-Audiences> [<https://perma.cc/WX6T-FDWT>].

⁶ Meta, *Ad Targeting: Help your ads find the people who will love your business*, <https://www.facebook.com/business/ads/ad-targeting> [<https://perma.cc/DU6C-UHFV>].

23. The Meta Pixel (or, “the Pixel”), originally called the Facebook Pixel, was first introduced in 2015.⁷ It is now a primary means through which Meta acquires personal information to create customized audiences for its advertising business, although Meta’s public-facing descriptions of the Pixel obscure and minimize this fundamental purpose of the tracking code. Instead, Meta characterizes the Pixel as a simple “snippet of JavaScript code” that helps website owners keep track of user activity on their websites.⁸ Meta emphasizes that website managers can set up the Pixel easily, without any help from their web developer. “You only need to place a single pixel across your entire website.”⁹ The Pixel is installed on an estimated 30 percent of popular internet websites.¹⁰

24. The Meta Pixel sends Meta volumes of information about each visit to each website where it is embedded. Regardless of the purpose (if any) a website owner may have for allowing the Meta Pixel to function on its webpages, the code is configured to capture a substantial amount of information by default, with additional options permitting a website operator to collect even more data.

25. In 2018, Meta introduced a “first-party cookie option” for the Pixel, to circumvent improvements in how web browsers block third-party cookies (a primary means by which

⁷ Cecile Ho, Meta, *Announcing Facebook Pixel* (Oct. 14, 2015), <https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/> [<https://perma.cc/M7XS-2LEJ>].

⁸ Meta for Developers, *Meta Pixel*, <https://developers.facebook.com/docs/meta-pixel/> [<https://perma.cc/BE7F-K93P>]; Meta, *Retargeting: Inspire People to Rediscover What They Love About Your Business*, <https://www.facebook.com/business/goals/retargeting> [<https://perma.cc/M3DG-8YN4>] (Meta Pixel “tracks the people [who visit your website] and the type of actions they take.”)

⁹ *Announcing Facebook Pixel*, *supra* n.7.

¹⁰ Maria Puertas and Simon Fondrie-Teitler, The Markup, *In 2023, Resolve to Fix Your Organization’s Meta Pixel Problem* (Jan. 31, 2023), <https://themarkup.org/levelup/2023/01/31/in-2023-resolve-to-fix-your-organizations-meta-pixel-problem> [<https://perma.cc/89JD-8RL5>].

Facebook historically tracked people across the web).¹¹ Being embedded in websites as a first-party cookie, rather than as a third-party cookie, causes users' browsers to treat that Pixel as though it is offered by the website they are visiting, rather than by Meta, a third party. When the Pixel is embedded in a website as a first-party cookie, the third-party cookie blocking functions of modern web browsers do not inhibit the Meta Pixel's collection of data.

26. In short, circumventing privacy measures designed to protect users' information, the Meta Pixel consistently captures HTTP headers, Pixel-specific data, and Button Click data on every visit to every website through its default operation. Meta acknowledges that the Pixel is configured to collect this information, and can collect the following non-exhaustive categories of information from the webpages where it is embedded:

Http Headers – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and person using the website.

Pixel-specific Data – Includes Pixel ID and the Facebook Cookie.

Button Click Data – Includes any buttons clicked by site visitors, the labels of those buttons and any pages visited as a result of the button clicks.

Optional Values – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.

Form Field Names – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.¹²

¹¹ Sergiu Gatlan, Softpedia News, *Facebook to Circumvent Cross-Site Tracking Block with New First-Party Cookie* (Oct. 6, 2018), <https://news.softpedia.com/news/facebook-to-circumvent-cross-site-tracking-block-with-new-first-party-cookie-523089.shtml> [<https://perma.cc/KR3H-PY5P>].

¹² *Meta Pixel*, supra n.8; see also Meta for Developers, *Meta Pixel: Advanced*, <https://developers.facebook.com/docs/facebook-pixel/advanced/> [<https://perma.cc/M3EA-LHVM>]; Meta Business Help Center, *Best practices for Meta Pixel setup*, <https://www.facebook.com/business/help/218844828315224?id=1205376682832142> [<https://perma.cc/SU7N-XGFL>]; Meta for Developers, *App Events API*, <https://developers.facebook.com/docs/marketing-api/app-event-api/> [<https://perma.cc/NV4L->

27. While certain features are included in the Pixel by default, Meta also allows companies like Labcorp to intentionally modify those default settings to allow for the interception and disclosure of additional data about its website users. As seen in the network traffic below from Labcorp's website highlighted in yellow, Labcorp purposely modified the Pixel settings to include fields such as "Automatic Matching," "Prohibited Sources," and "UnwantedData":

```
fbq.loadPlugin("cookie");
instance.optin("131376945570139", "FirstPartyCookies", true);
fbq.loadPlugin("automaticmatchingforpartnerintegrations");
instance.optin("131376945570139", "AutomaticMatchingForPartnerIntegrations", true);
config.set(null, "batching", {"batchWaitTimeMs":501,"maxBatchSize":10});
config.set(null, "microdata", {"waitTimeMs":500});
config.set("131376945570139", "prohibitedSources", {"prohibitedSources":{}});
fbq.loadPlugin("prohibitedsources");
instance.optin("131376945570139", "ProhibitedSources", true);
config.set("131376945570139", "unwantedData", {"blacklisted_keys":{"PageView":{"cd":["lat","lon","firstName","lastName","?lat","firstName","lastName","client_ip"]},"sensitive_keys":{"CustomizeProduct":{"cd":["url"]},"AddToWishlist":{"cd":["url"]},"a7266514d7714e38d9eb63a18ea812fad9bae24909966f5a4340a7cd91936ae3","a8b771920b8319e47251d1360f5e880bc18e8d329b0f0d003ea3c7e615558947"},"PageVieww":{"cd":["url"]},"8e35c2cd3bf6641bdb0e2050b76932cbb2e6034a0ddacc1d9bea82a6ba57f7cf","d75dce204e8621ca939afebd30181047e29a3ed8bb5e89a4ed150e820346c07","a8b771920b8319e47251d1360f5e880bc18e8d329b0f0d003ea3c7e615558947","ba1a4a7396c977512f14acd59b4c40784c50a1dd63dcb437705dd67e76f7c96","bc06218919372b0017b72bc984fb150ac561f2a7097cf69997c0721b2008de","037aeaeaf4bbf26ddabe7256a8294dc52da48d575a1247b5c2598c47de7aebab","52cb14ab57148fc6ee6e582bbec720db2fbc23b83efa51e07581380d5b66c978","ce4e9a0dad1eed8d69c713692a749e6b6c486f79156eca3c2e9ae6db22b633e6"},"FindLocation":{"cd":["url"]},"a8b771920b8319e47251d1360f5e880bc18e8d329b0f0d003ea3c7e615558947","8e35c2cd3bf6641bdb0e2050b76932cbb2e6034a0ddacc1d9bea82a6ba57f7cf","8f84b89bd c2aa18af73a15328a4761e8d85051000282224d06cef0111c961b","a7266514d7714e38d9eb63a18ea812fad9bae24909966f5a4340a7cd91936ae3","ce4e9a0dad1eed8d69c713692a749e6b6c486f79156eca3c2e9ae6db22b633e6"},"Donate":{"cd":["url"]},"a7266514d7714e38d9eb63a18ea812fad9bae24909966f5a4340a7cd91936ae3","a8b771920b8319e47251d1360f5e880bc18e8d329b0f0d003ea3c7e615558947"}));
fbq.loadPlugin("unwanteddata");
instance.optin("131376945570139", "UnwantedData", true);
fbq.loadPlugin("iabpcmaebridge");
instance.optin("131376945570139", "IABPCMAEBridge", true);
config.set("131376945570139", "browserProperties", {"delayInMs":200,"enableEventSuppression":true,"enableBackupTimeout":true});
fbq.loadPlugin("browserproperties");
instance.optin("131376945570139", "BrowserProperties", true);
config.set("131376945570139", "protectedDataMode", {"standardParams":{
  "lead_event_source":true,"predicted_itv":true,"product_catalog_id":true,"availability":true,"body_style":true,"checkin_date":true,"checkout_date":true,"city":true,"condition_of_vehicle":true,"content_category":true,"content_ids":true,"content_name":true,"content_type":true,"contents":true,"country":true,"currency":true,"delivery_category":true,"departing_arrival_date":true,"departing_departure_date":true,"destination_airport":true,"destination_ids":true,"dma_code":true,"drivetrain":true,"exterior_color":true,"fuel_type":true,"hot_el_score":true,"interior_color":true,"lease_end_date":true,"lease_start_date":true,"listing_type":true,"make":true,"mileage.unit":true,"mileage.value":true,"model":true,"neighborhood":true,"num_adults":true,"num_children":true,"num_infants":true,"num_items":true,"order_id":true,"origin_airport":true,"postal_code":true,"preferred_baths_range":true,"preferred_beds_range":true,"preferred_neighborhoods":true,"preferred_num_stops":true,"preferred_price_range":true,"preferred_star_ratings":true,"price":true,"property_type":true,"region":true,"returning_arrival_date":true,"returning_departure_date":true,"search_string":true,"state_of_vehicle":true,"status":true,"suggested_destinations":true,"suggested_home_listings":true,"suggested_hotels":true,"suggested_jobs":true,"suggested_local_service_businesses":true,"suggested_location_based_items":true,"suggested_vehicles":true,"transmission":true,"travel_class":true,"travel_end":true,"travel_start":true,"trim":true,"user_bucket":true,"value":true,"vin":true,"year":true});
fbq.loadPlugin("protecteddatamode");
instance.optin("131376945570139", "ProtectedDataMode", true);
config.set("131376945570139", "ccRuleEvaluator", {"ccRules":{"id":"667622770915547","rule":{"and":[{"event":{"eq":"PageView"}},{or":{"URL":{"i_contains":"https://www.labcorp.com/Vcoronavirus-disease-covid-19/providers"}}]}},{id":"328998115902461","rule":{"and":[{"event":{"eq":"PageView"}},{or":{"URL":{"i_contains":"https://www.labcorp.com/Vcoronavirus-disease-covid-19/individuals/convenient-infection-test-options"}}]}},{id":"3696856433750934","rule":{"and":[{"event":{"eq":"PageView"}},{or":{"URL":{"i_contains":"https://www.labcorp.com/Vlabs-and-appointments"}}]}},{wcaRules":{"rule":{"and":[{"event":{"eq":"InitiateCheckout"}},{id":"8263448550395147"}},{rule":{"and":[{"event":{"eq":"ViewContent"}},{id":"5594995463924889"}},{rule":{"and":[{"event":{"eq":"AddToCart"}},{id":"5657781124298348"}},{rule":{"and":[{"event":{"eq":"Purchase"}},{id":"5604211286281843"}},{rule":{"and":[{"event":{"eq":"ViewContent"}},{id":"7899129856771294"}},{rule":{"and":[{"event":
```

XM9S]; Meta for Developers, *Meta Pixel: Get Started*, <https://developers.facebook.com/docs/meta-pixel/get-started> [<https://perma.cc/5W4A-SKGP>].

Among other things, the Automatic Matching feature helps Meta match website users to Meta Pixel “events” (i.e., actions taking place on Labcorp’s website).¹³ Meta is explicit that Automatic Matching must be turned on by website developers like Labcorp.¹⁴

28. In all websites where the Pixel operates, when a user exchanges information with the host of that site—such as through a search query—Meta’s software script surreptitiously directs the user’s browser to send a separate message to Meta’s servers. This second, secret transmission contains the original request sent to the host website, (“GET request”), along with additional data that the Pixel is configured to collect (“POST request”).¹⁵ GET and POST requests are communications that contain contents from both the user and from servers associated with the website they are visiting. These transmissions are initiated by Meta code and concurrent with the communications to and from the host website.

29. Meta associates the information it obtains via the Meta Pixel with other information regarding the user, using personal identifiers that are transmitted concurrently with other information the Pixel is configured to collect. For Facebook account-holders, these identifiers include the “c_user” IDs, which allow Meta to link data to a particular Facebook account, and “xs” cookies associated with a browsing session. For both Facebook account-holders and users who do not have a Facebook account, these identifiers also include cookies that Meta ties to their browser, such as “datr” and “fr” cookies.¹⁶

¹³Meta Business Help Center, *About advanced matching for web*, <https://www.facebook.com/business/help/611774685654668?id=1205376682832142> [https://perma.cc/65LM-Z9R8]

¹⁴ See *id.* (“To set up automatic advanced matching, you don't need to code. You can toggle it on in Meta Events Manager.”).

¹⁵ Surya Mattu et al., The Markup, *How We Built a Meta Pixel Inspector* (Apr. 28, 2022), <https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector> [https://perma.cc/S7PB-WCWX]

¹⁶ Meta, *Cookies Policy* (Oct. 5, 2022), <https://www.facebook.com/policy/cookies> [https://perma.cc/6M55-KWA4].

30. The “c_user” ID labelled in Meta’s software script reveals a Facebook account-holder’s Facebook ID (“FID”). A subscriber’s FID is a unique sequence of numbers linked to that individual’s Facebook profile. Entering “facebook.com/[FID]” into a web browser returns the Facebook profile of that particular person. A FID thus identifies a person more precisely than a name.

31. Meta informs website managers that, among other things, the Pixel allows “you...to track Facebook ad-driven visitor activity on your website...[and] use the data to analyze your website’s conversion flows and optimize your ad campaigns.”¹⁷

32. Meta feeds the vast quantities of information obtained from the Pixels into its advertising systems, using it to identify users and their personal characteristics, categorize them for Meta’s business purposes, and target them with marketing messages from its advertising clients.

33. Meta acknowledges this use of data acquired through the Pixel tracking code. For example, Meta refers to the Pixel as one of Meta’s “Business Tools,” and to websites with the Pixel embedded as “Partners.” Meta explains in its Privacy Policy, among other places, that Meta uses “[i]nformation from Partners,” expressly including information about “[w]ebsites you visit and cookie data,” “to provide a personalized experience to [users], including ads.”¹⁸

34. One of the ways that Meta uses data obtained via the Pixel for advertising is by using it to define “audiences” customized for particular advertisers. Meta sells access to three types of tailored audiences.

¹⁷ Meta, *Get Started*, <https://developers.facebook.com/docs/meta-pixel/get-started> [<https://perma.cc/5W4A-SKGP>].

¹⁸ Meta Privacy Center, *Privacy Policy* (Effective June 15, 2023), <https://www.facebook.com/privacy/policy> [<https://perma.cc/CA25-2MKT>].

35. Advertisers can purchase access to “Core Audiences,” composed of individuals with specified traits and characteristics. Meta assigns users to Core Audiences based on data it has learned or inferred (including via data from the Pixel) about a range of their personal qualities, including users’ location, age, gender, education, job title, connections to other Facebook users or pages, interests and hobbies, and behavior such as prior purchases and device usage.¹⁹

36. Meta also sells access to “Custom Audiences,” meaning the ability to reach “people who have already shown interest in [an advertiser’s] business, whether they’re loyal customers or people who have used [their] app or visited [their] website.”²⁰ Meta assigns users to Custom Audiences based on information from the Meta social media platform, and/or information the advertiser discloses about those users, such as e-mail subscriber lists, and activity tracked on the advertiser’s website(s), including via the Pixel.²¹

37. Meta also sells access to “Lookalike Audiences,” a Meta feature that “leverages information such as demographics, interests and behaviors from your source audience [i.e., a Custom Audience tailored from the advertiser’s records] to find new people who share similar qualities” with existing customers or Custom Audiences.²² To generate Lookalike Audiences, Meta uses data it has obtained from across the web, including from the Pixels embedded in third-

¹⁹ *Ad targeting, supra* n.6.

²⁰ *Id.*

²¹ Meta Business Help Center, *Create a customer List Custom Audience*, <https://www.facebook.com/business/help/170456843145568?id=2469097953376494> [<https://perma.cc/9M5M-VLTA>]; see also Adespresso, *Facebook Custom Audiences 101: The Complete Guide for Marketers* (Mar. 23, 2021), <https://adespresso.com/blog/facebook-ads-custom-audiences-guide/> [<https://perma.cc/NL29-3QP3>].

²² Meta Business Help Center, *About lookalike audiences*, <https://www.facebook.com/business/help/164749007013531?id=401668390442328> [<https://perma.cc/S5T3-99MP>].

party websites that have no relationship with the advertiser requesting access to a Lookalike Audience.

C. Google Analytics

38. Alphabet Inc., the parent holding company of Google, generates revenues primarily by delivering targeted online advertising through Google, which is the creator of the Google Source Code and an established advertising company.

39. Google Source Code—the source code associated with Google’s advertising system and products, including Google Analytics—is designed to track and collect individuals’ information when they are browsing the Internet.

40. Google Analytics is associated with the domains www.Google-Analytics.com and analytics.google.com.

41. Google Source Code is provided by Google in a copy-and-paste format and its functionality is uniform on all web properties, with the option for companies like Labcorp to choose to disclose additional data about its users to Google. Its operation is hidden by Google’s design and does not indicate to users that Google Source Code is present on a website they are visiting.

42. When the Google Source Code is placed by a company such as Labcorp on its website (<https://www.labcorp.com/>), Labcorp’s actions allow the Google Source Code to instruct the computer accessing Labcorp’s home page to track, intercept, and redirect the user’s information to Google.

43. This tracking, interception, and redirection of information occurs when individuals exchange communications or requests with the relevant websites.

44. Google Analytics, a marketing tool used for advertising and analytics, is one of Google’s primary products and services that leverage Google Source Code to track, collect, and

subsequently use (i.e. monetize) individuals' personal information. A fundamental and primary purpose of Google Analytics is to obtain the information about consumers' communications and activities that is accessible by entities other than Google. Google accomplishes this through Google Analytics, in part, by touting it as a tool that enables clients to "understand the customer journey and improve marketing ROI."²³ Specifically, according to Google, Google Analytics is intended to help advertisers:

- a. "Unlock customer-centric measurement" to "[u]nderstand how your customers interact across your sites and apps, throughout their entire lifecycle;"
- b. "Get smarter insights to improve ROI," to "[u]ncover new insights and anticipate future customer actions with Google's machine learning to get more value out of your data;" and
- c. "Connect your insights to results," to "[t]ake action to optimize marketing performance with integrations across Google's advertising and publisher tools[.]"²⁴

45. Like the Meta Pixel, when a user exchanges information with the host of a website—such as through a search query—Google Source Code operates to surreptitiously directs the user's browser to send a separate message to Google's servers. This second, secret transmission contains the original request sent to the host website, ("GET request"), along with additional data that the Google Source Code is configured to collect ("POST request). These transmissions are initiated by Google Source Code and concurrent with the communications to and from the host website.

²³ Google Marketing Platform, *Analytics*, <https://marketingplatform.google.com/about/analytics/> [<https://perma.cc/99GM-U3C5>]

²⁴ *Id.*

46. Google Analytics offers website developers like Labcorp the option to include additional data of their own choosing about its users' activities in any communications to Google, including "Event Value" and "Event Label" data. As can be seen from the Google Analytics developer website, this data is optional and not sent to Google by default²⁵:

Google Analytics > Measurement > Measurement Protocol (Universal Analytics)

Filter

Protocol Reference
Parameter Reference
Geographical IDs

Events

Event Category

Required for event hit type.
Specifies the event category. Must not be empty.

Parameter	Value Type	Default Value	Max Length	Supported Hit Types
ec	text	None	150 Bytes	event

Example value: Category
Example usage: `ec=Category`

Event Action

Required for event hit type.
Specifies the event action. Must not be empty.

Parameter	Value Type	Default Value	Max Length	Supported Hit Types
ea	text	None	500 Bytes	event

Example value: Action
Example usage: `ea=Action`

Event Label

Optional.
Specifies the event label.

Parameter	Value Type	Default Value	Max Length	Supported Hit Types
el	text	None	500 Bytes	event

Example value: Label
Example usage: `el=Label`

Event Value

Optional.
Specifies the event value. Values must be non-negative.

Parameter	Value Type	Default Value	Max Length	Supported Hit Types
ev	text	None	500 Bytes	event

On this page

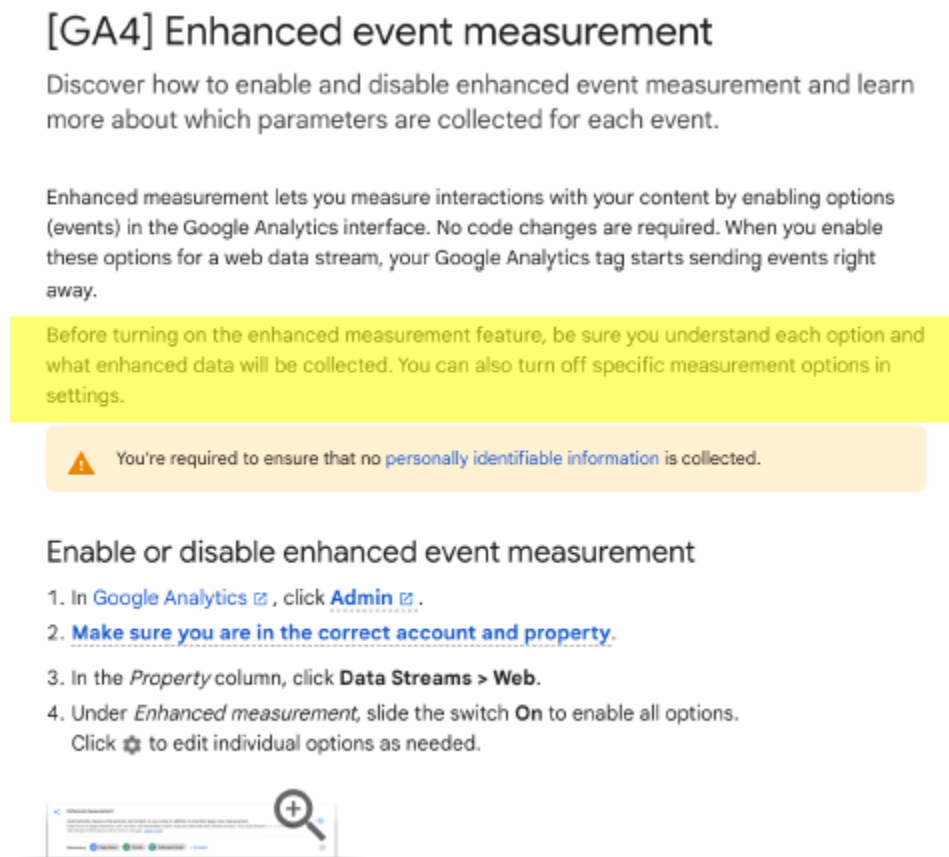
- General
- Protocol Version
- Tracking ID/ Web Property ID
- Mask IP
- Disabling Advertising Personalization
- Data Source
- Queue Time
- Cache Buster
- User
- Client ID
- User ID
- Session
- Session Control
- IP Override
- User Agent Override
- Geographical Override
- Traffic Sources
- Document Referrer
- Campaign Name
- Campaign Source
- Campaign Medium
- Campaign Keyword
- Campaign Content
- Campaign ID
- Google Ads ID
- Google Display Ads ID
- System Info
- Screen Resolution
- Viewport size
- Document Encoding
- Screen Colors
- User Language
- Java Enabled
- Flash Version
- Hit
- Hit type
- Non-Interaction Hit
- Content Information
- Document location URL
- Recommended for you
- Working with the Measurement Protocol
- Updated Jun 10, 2021
- Measurement Protocol Reference
- Updated Dec 4, 2020
- Validating Hits - Measurement Pr
- Updated Jun 10, 2021

47. Labcorp itself chose to configure Google Analytics to communicate this information about Labcorp website users, as seen below at paragraph 74, showing the transmission of the "el" (Event Label) and "ev" (Event Value) fields, which provide Google

²⁵ Google Analytics, *Measurement Protocol Parameter Reference*, <https://developers.google.com/analytics/devguides/collection/protocol/v1/parameters> [<https://perma.cc/TT6N-UXSF>].

with the search terms entered by a user into the search bar on Labcorp's home page (here, "pregnancy") and a test number for a urine pregnancy test that the user copied into the computer's clipboard.

48. In addition, upon information and belief, Labcorp chose to disclose search terms users entered into the Labcorp website to Google via Google Analytics by enabling the Google Analytics "Enhanced event measurement" feature:



In other words, Labcorp took affirmative, additional steps of its own to configure Google Analytics' tracking's ability to ensure that Google received additional data about its website users.

49. Also like the Meta Pixel, Google associates the information it obtains via Google Source Code with other information regarding the user, using personal identifiers that are

transmitted concurrently with other information the code is configured to collect. These identifiers include the “cid”, a combination of the time at which the user visited the website and a unique identifier. The “cid” is assigned to an individual’s browser and can persist for up to two years, allowing Google to link a series of events to the same browser and, thus, to an individual. For Google account-holders, this identifier is also linked to that account.

50. In addition to information gleaned from a user’s “cid,” Google can create a unique, digital “fingerprint” for a user based on data transmitted via Google Source Code, which allows Google to link certain web activity to a user. This “fingerprint” can consist of information regarding a user’s screen depth, screen resolution, browser name and version, and operating system name and version, as well as a user’s Internet Protocol (“IP”) address. With that information, Google is able to link data acquired through Google Analytics to a particular user.

51. After tracking, intercepting, and acquiring user’s information, Google uses the information for personalized advertising in its advertising systems which includes, but is not limited to, Google Analytics.

52. For example, Google Analytics uses the information it collects to facilitate its Audience Targeting feature. Audience Targeting refers to serving ads to only a select number of users who share certain common characteristics. For Google’s Audience Targeting, Google can target ads to either “Pre-defined Google Audiences” or “Advertiser-curated Audiences.” Pre-defined Audiences are those created by Google based on interest and demographic data. Advertiser-curated Audiences are customized audiences created by Google through the use of the Source Code, including audiences created through Google Analytics.

53. Like Meta, Google is therefore able to monetize the information it surreptitiously intercepts from visitors to the Labcorp website.

IV. Third Parties Obtain Sensitive Personal Information From Labcorp

54. Labcorp's website, <https://www.labcorp.com>, permits individuals to access their medical testing results, book medical testing appointments, request medical testing supplies, and pay for Labcorp services they have received.

55. Individuals can also use the Labcorp website's search bar to look for medical information, including information concerning specific medical tests.

56. Labcorp embedded and configured the Meta Pixel, Google Analytics, and other Third-party Tracker code on the Labcorp website during the relevant period and transmitted extensive information regarding visitors to Labcorp website's homepage to specific third parties. The information transmitted included the identities of individuals visiting the website, health-related information and inquiries (including searches made on the website), and webpages visited as a result of those inquiries.

57. These third parties, including Facebook and Google, intentionally obtain confidential communications subject to the protections of CIPA and WESCA between the Labcorp website and users of that website.

58. Labcorp's implementation of and configuration of these Third-party Trackers' code on its website permitted the Third Party-Trackers to intercept and use Plaintiffs' and Class members' data, including identifiable and sensitive health information. And as described above, Labcorp took affirmative steps to configure the Meta Pixel and Google Analytics trackers to permit the disclosure of even more information to Meta and Google about its website users.

A. Labcorp Facilitated the Disclosure of Labcorp Website Users' Communications to Meta Via the Meta Pixel.

59. Labcorp facilitated the disclosure to Meta of – in a single transmission – (i) the search terms Plaintiffs and Class members entered into the search bar on Labcorp homepage; (ii) the Facebook ID (or FID); and (iii) the title of the Labcorp webpage visited as a result of that search query. This data transmission is depicted immediately below:

[illegible]

60. In this example, the intercepted URL contains the title of the Labcorp webpage visited, “cancer colorectal patient,” as evidence by the “path” visible in the code:

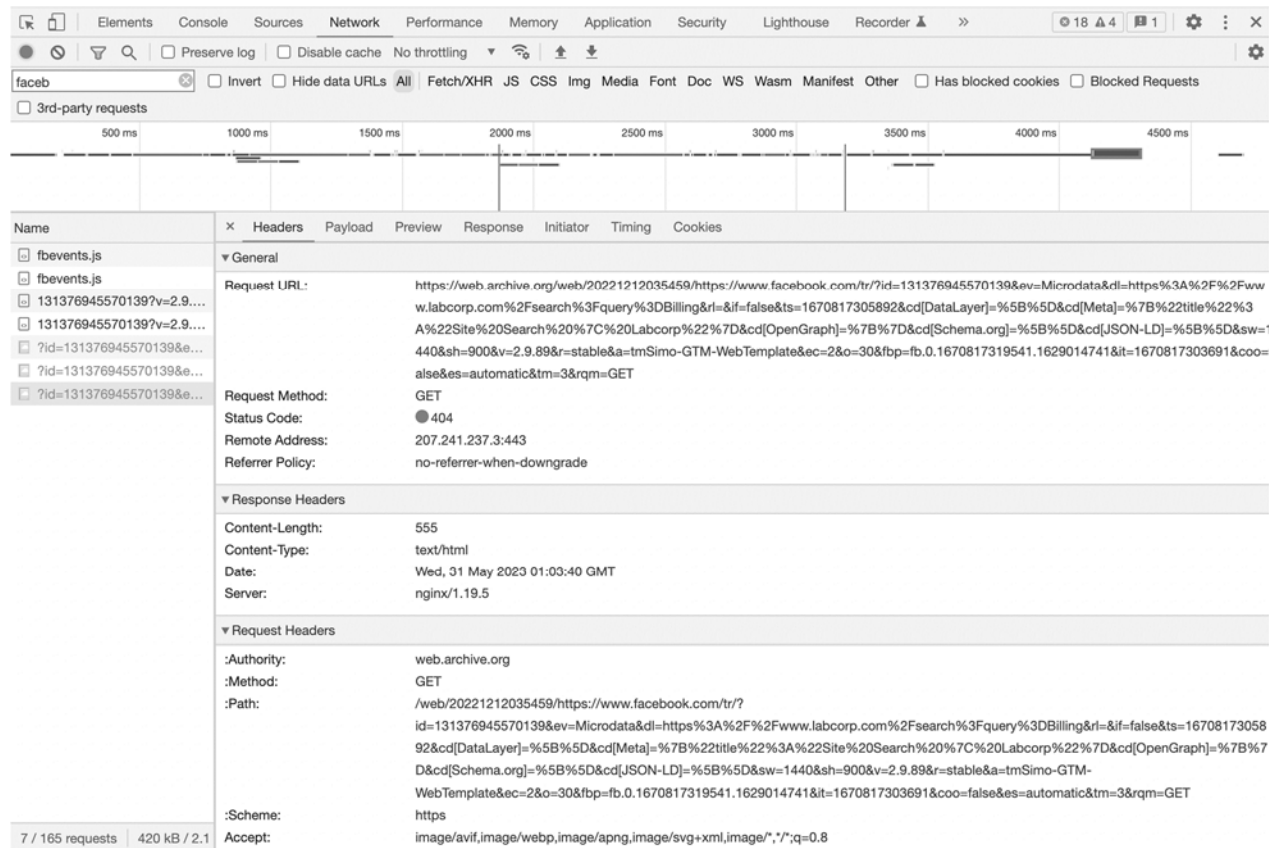
```
:method: GET  
:path: /tr/?id=715864809660919&v-Microdata&d1=https%3A%2F%2Fwww.labcorp.com%2F%3Fcolorectal%2Fpatient%  
s&r1=https%3A%2F%2Fwww.labcorp.com%2F&if=false&ts=1672328826546&cd[DataLayer]=-%S%SD&cd[Meta]=-%7B%22title%2  
2%3A%22Colorectal%20Cancer%2BScreening%20and%20Information%20%7C%20Labcorp%22%2C%22meta%3Adescription%22%3  
A%22Routine%20screenings%20significantly%20reduce%20the%20odds%20of%20colon%20cancer%20impacting%20you%20an  
d%20your%20family.%20The%20Labcorp%20OnDemand%20Colon%20Cancer%20FIT%20Kit%20may%20make%20sense%20for%20yo  
u.%22%7D&cd[OpenGraph]=-%7B%7D&cd[Schema.org]=-%S%SD&cd[JSON-LD]=-%S%SD&sw=95&sh=874&v=2.9.90&r=stable&a=ts  
Simo-GTM-WebTemplate&c=1&o=30&fbp=fb.1.1671141355107.1533100921&it=1672328821166&coo=false&dpo=LDU&dpo-co=  
&dpost=0&es=automatic&ts=3&rqn=GET  
:scheme: https
```

61. The FID is displayed in the “c_user” code. In this example, the code is redacted to preserve the privacy of the user:

```
cache-control: no-cache
cookie: sb=QTUSYyU59F9rwxDEEHQ4cOd; datr=QTUSY917xR64J5k8mvyb-uPc; c_user=[REDACTED]; dpr=0.833333373069763
2; xs=6X3AmajjXGt5p1yYbAX3A23A16624853973A-1%3A24253A3A3AAcXofOpcLpdudk-rzna8FSZSR28IcxIhNvbpecDHPcc; fr
=8dQDuE1YVfS0lxYnP.AkU6Q4A1X-TnUrTpzjMUB56HsB4.BjrzNU.CZ.AAA.0.0.BjranN.AkUPyr-gQrs
pragma: no-cache
```

62. Meta (or anyone) can identify the user conducting that search by entering “facebook.com/” followed by the FID into their browser bar.

63. As indicated above, Labcorp also aided in the disclosure of a user’s search query string or the search terms entered on Labcorp’s homepage, which were transmitted to Meta in a single transmission as shown below:



64. In this example, the intercepted URL contains a user’s search query string or the search terms “billing” that was entered on Labcorp’s homepage, as evidenced by the “path” visible in the code:

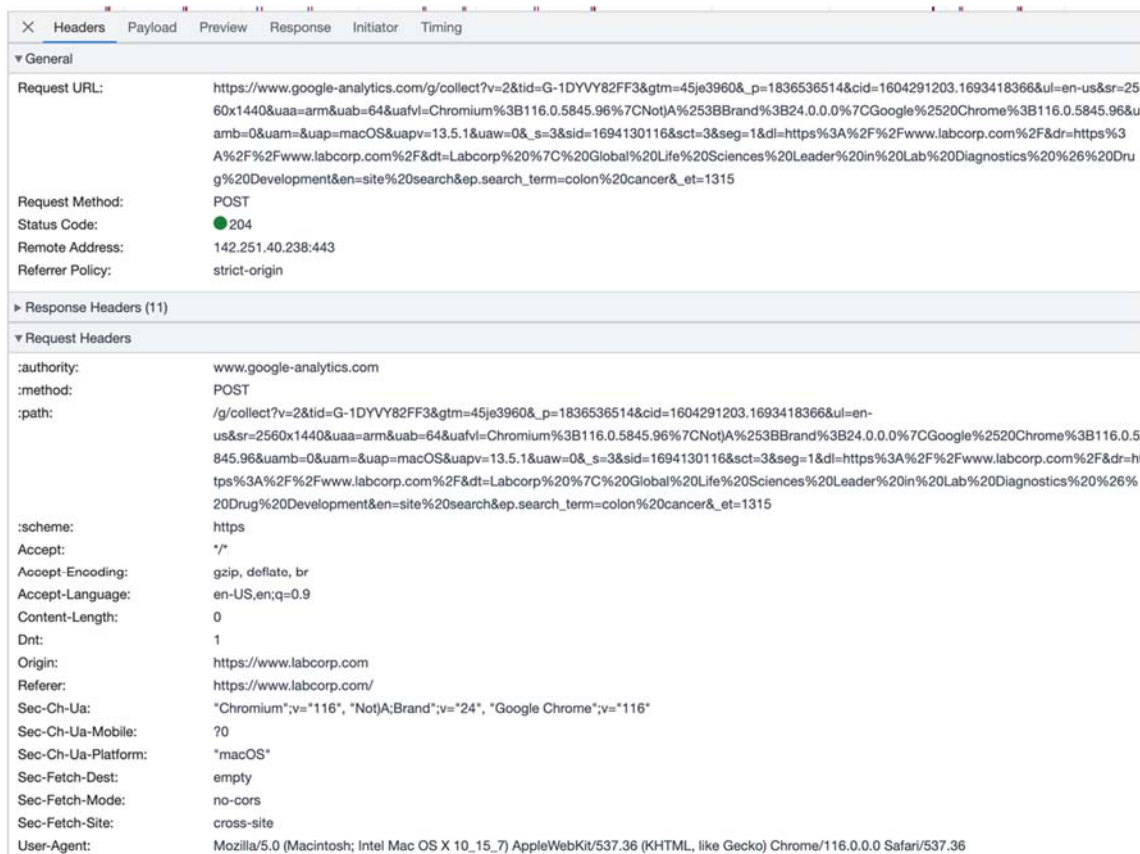
```

:Method: GET
:Path: /web/20221212035459/https://www.facebook.com/tr/?
id=131376945570139&ev=Microdata&dl=https%3A%2F%2Fwww.labcorp.com%2Fsearch%3Fquery%3DBilling&rl=&if=false&ts=16708173058
92&cd[DataLayer]=%5B%5D&cd[Meta]=%7B%22title%22%3A%22Site%20Search%20%7C%20Labcorp%22%7D&cd[OpenGraph]=%7B%7
D&cd[Schema.org]=%5B%5D&cd[JSON-LD]=%5B%5D&sw=1440&sh=900&v=2.9.89&r=stable&a=tmSimo-GTM-
WebTemplate&ec=2&o=30&fbp=fb.0.1670817319541.1629014741&it=1670817303691&coo=false&es=automatic&tm=3&rqm=GET
:Scheme: https

```

B. Labcorp Also Facilitates the Disclosure of Labcorp Website Users' Communications to Google Via Google Analytics

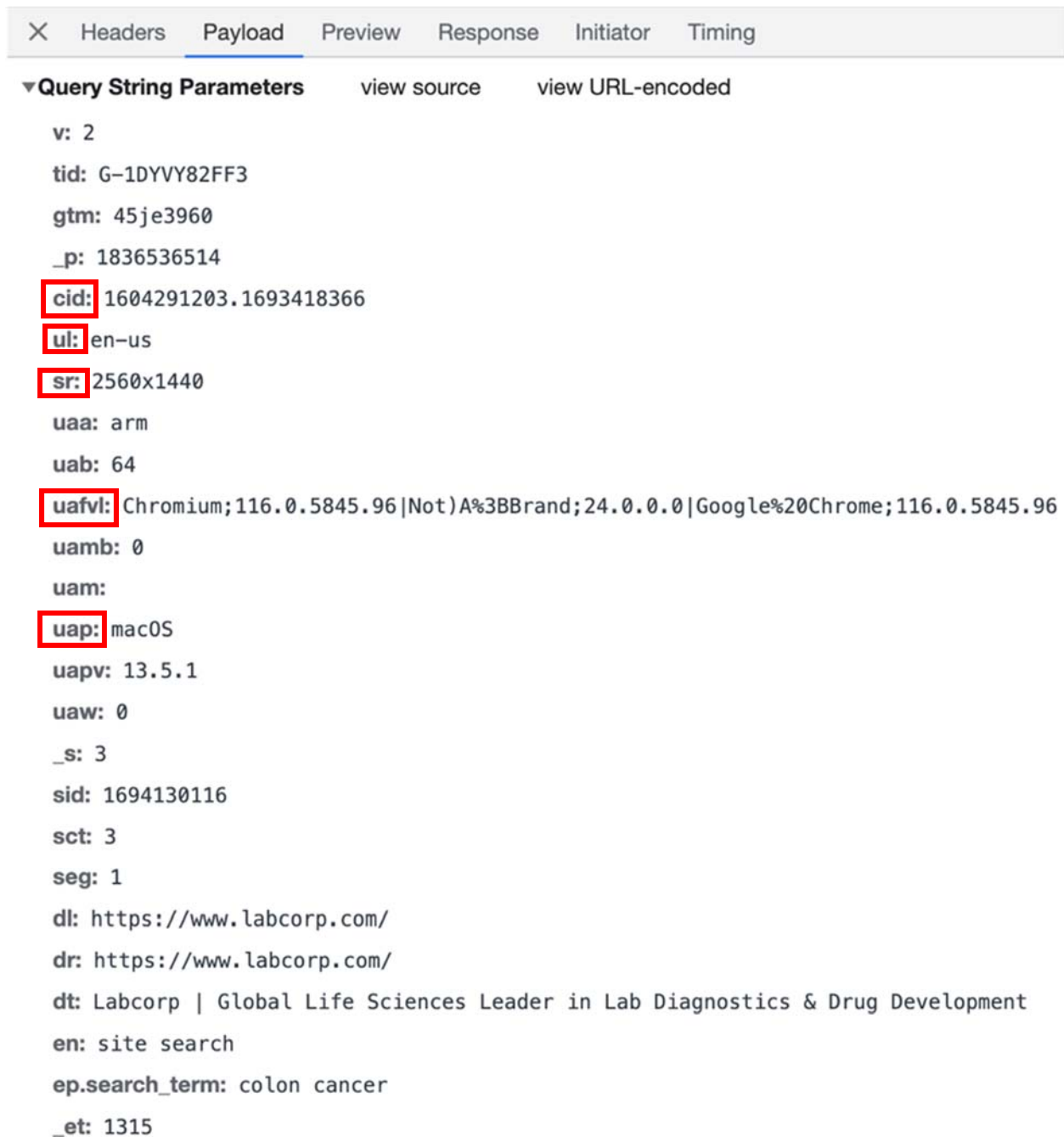
65. Labcorp also facilitates the disclosure of the same kinds of website user information to Google via Google Analytics that it discloses to Meta via the Meta Pixel. This includes a user's search query string or the search terms entered on Labcorp's homepage in a single transmission, as depicted below:



66. In this example, the intercepted URL contains a user's search query or the search terms "colon cancer" that was entered on Labcorp's homepage, as evidenced by the "path" visible in the code:

```
:method: POST
:path: /g/collect?v=2&tid=G-1DYVY82FF3&gtm=45je3960&p=1836536514&cid=1604291203.1693418366&ul=en-us&sr=2560x1440&uaa=arm&uab=64&uafvl=Chromium%3B116.0.5845.96%7CNot(A%253BBrand%3B24.0.0.0%7CGoogle%2520Chrome%3B116.0.5845.96&uamb=0&uam=&uap=macOS&uapv=13.5.1&uaw=0&s=3&sid=1694130116&sct=3&seg=1&dl=https%3A%2F%2Fwww.labcorp.com%2F&dr=https%3A%2F%2Fwww.labcorp.com%2F&dt=Labcorp%20%7C%20Global%20Life%20Sciences%20Leader%20in%20Lab%20Diagnostics%20%26%20Drug%20Development&en=site%20search&ep.search_term=colon%20cancer&_et=1315
:scheme: https
```

67. The “cid”— a combination of the time at which the user visited the website and a unique identifier linked to an individual’s browser and, if applicable, an individual’s Google account—is also transmitted in this disclosure, as depicted below:



68. In addition to a user’s “cid,” Google Source Code transmits information that can be used to create a unique, digital “fingerprint” for a user with which Google is able to link data acquired through Google Analytics to a particular user. In the example immediately above, this information includes, *inter alia*, the user’s language (“ul”), screen resolution (“sr”), operating system (“uap”), operating system version (“uapv”), and full information about the user’s web browser (“uafvl”).

69. Labcorp not only facilitates disclosures to Google of a user’s search query, but also any of the hyperlinks yielded by that search a user chooses to click.

70. In the following example, a user’s search for “colon cancer” on Labcorp’s website yielded a link to an article entitled, “The earlier the better: colon cancer screenings,” as well as information regarding MLH1 Promoter Methylation Analysis, a medical test.

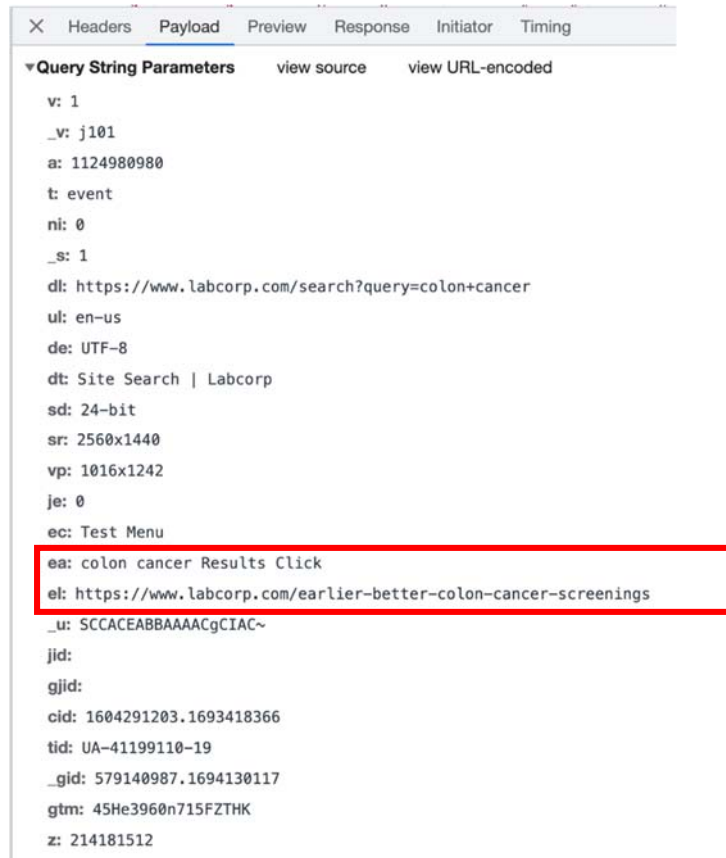
The screenshot shows the Labcorp website with a search bar containing "colon cancer". The search results are divided into two main sections: "Search Results" and "Test Menu Results".

Search Results: The first result is "The earlier the better: [Colon cancer](#) screenings", which is highlighted with a red box. Below it are several other links related to colon cancer screenings and tests.

Test Menu Results: This section displays a table of 21 test results found for "colon cancer". The first result, "MLH1 Promoter Methylation Analysis", is highlighted with a red box. The table includes columns for Number, Name, Specimen, and New or Updated.

Number	Name	Specimen	New or Updated
512031	MLH1 Promoter Methylation Analysis	Formalin-fixed, paraffin-embedded (FFPE) tissue block or slides	>
511654	EPCAM Deletion / Duplication Analysis	Whole blood	>
164119	Bowel Disorders Evaluation Rule-out Cascade	Serum	>
081950	Vitamin D, 25-Hydroxy	Serum	>

71. If a user accesses that article by clicking on the associated hyperlink, Labcorp discloses that action to Google.

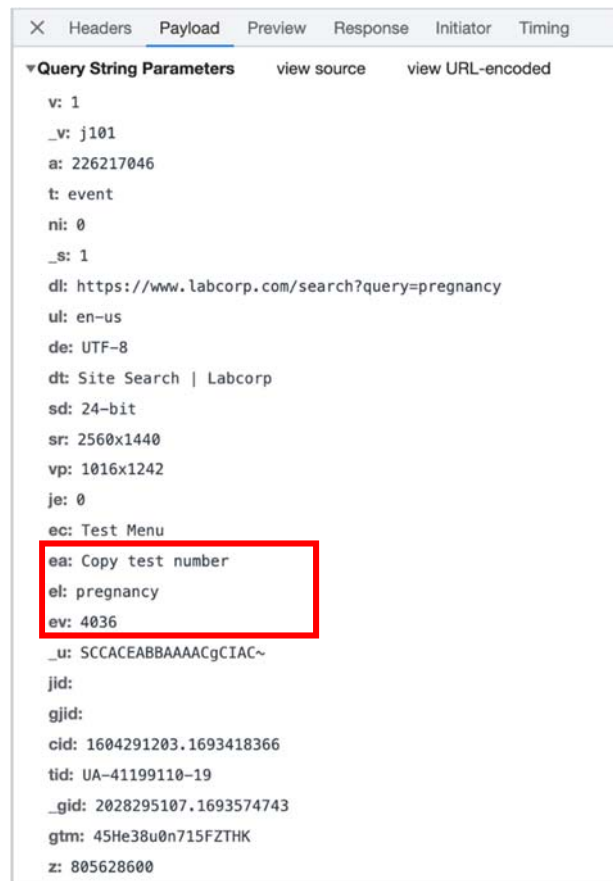


72. Similarly, if a user seeks more information regarding the above-mentioned medical test, which appears as a hyperlink after the user conducts an initial search in Labcorp's search bar, Labcorp also discloses that action to Google as well:

```
X Headers Payload Preview Response Initiator Timing
▼ Query String Parameters view source view URL-encoded
v: 1
_v: j101
a: 792537903
t: event
ni: 0
_s: 1
dl: https://www.labcorp.com/search?query=colon+cancer
ul: en-us
de: UTF-8
dt: Site Search | Labcorp
sd: 24-bit
sr: 2560x1440
vp: 1016x1242
je: 0
ec: Test Menu
ea: colon cancer Results Click
el: /tests/512031/i-mlh1-i-promoter-methylation-analysis
_u: SCCACEABBAACgCIAC~
jid:
gid:
cid: 1604291203.1693418366
tid: UA-41199110-19
_gid: 2028295107.1693574743
gtm: 45He38u0n715FZTHK
z: 295921077
```

73. Labcorp also discloses to Google if a user otherwise indicates interest in a medical test by “copying” the test number to the computer’s clipboard, a common tool that temporarily stores text or other data.

74. In the following example, a user's search for "pregnancy" on Labcorp's website yielded a link to a test for a urine pregnancy test. When a user copies the relevant "test number" onto the computer's clipboard, Labcorp also discloses that action to Google:



75. Labcorp also has embedded and configured code on its website that allows third parties other than Meta and Google to intercept a user's search query string. Those third parties include Algolia, Eloqua, Adsrvr, and Qualtrics.

76. Plaintiffs and members of the proposed Classes did not authorize Meta, Google, or any other third party to obtain the content of communications between them and Labcorp, including to review or use this data for advertising or any other purpose. The wide-ranging and near-constant acquisition of sensitive content, such as medically-related search queries, from communications between Plaintiffs/Class members and Labcorp violates CIPA and WESCA.

77. Labcorp users are provided no indication that Meta, Google, or any other third parties intercept this data, or that Labcorp facilitated or procured the interception of the same.

TOLLING, CONCEALMENT, AND ESTOPPEL

78. The statutes of limitation applicable to Plaintiffs' claims are tolled as a result of Defendants' knowing and active concealment of their conduct alleged herein.

79. Among other things, Defendants affirmatively hid their true actions and knowingly made statements that were misleading and concealed the true nature of their conduct and operation. The circumstances of third-party trackers employed on and with respect to the Labcorp website would lead reasonable users to believe third parties were not collecting their personal information or that Labcorp was facilitating disclosure of the same.

80. Moreover, Plaintiffs were ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their own part.

81. Furthermore, under the circumstances Defendants were under a duty to disclose the true character, quality, and nature of its activities to Plaintiffs. Defendants therefore are estopped from relying on any statute of limitations.

82. All applicable statutes of limitation also have been tolled by operation of the discovery rule. Specifically, Plaintiffs and other Class members could not have learned through the exercise of reasonable diligence of Defendants' conduct as alleged herein.

PLAINTIFF SPECIFIC ALLEGATIONS

83. Plaintiff Howard is a California resident who visited the Labcorp website (<https://www.labcorp.com/>) in or around December 2022 to conduct searches on the website regarding a variety of sensitive medical issues.

84. Ms. Howard conducted these searches on the Labcorp website from a web browser while in California.

85. Ms. Howard has had a Facebook and/or Meta account since approximately July 2011 and a Google account for over a decade.

86. Each time Meta, Google, and other third parties obtained Ms. Howard's identifying information and the searches she conducted on the Labcorp website, it violated her rights under CIPA. These third parties obtained this information because Labcorp embedded and configured their computer code on its website to surreptitiously track and disclose communications between Ms. Howard and Labcorp.

87. Meta, Google, and other third-parties intercepted Ms. Howard's private information in California after Labcorp embedded and configured their computer code on its website for the purpose of collecting private information from users such as Ms. Howard routed that information to third parties through Ms. Howard's browser.

88. Ms. Howard never consented to the interception of this private information or Labcorp's facilitation of the same.

89. Plaintiff Hernandez is a California resident who visited the Labcorp website (<https://www.labcorp.com/>) beginning in or around October 2022 and continuing through approximately December 2022 to conduct searches on the website regarding a variety of sensitive medical issues.

90. Ms. Hernandez conducted these searches on the Labcorp website from a web browser while in California.

91. Ms. Hernandez has had a Facebook and/or Meta account since 2009 and a Google account for at least five years.

92. Each time Meta, Google, and other third parties obtained Ms. Hernandez's identifying information and the searches she conducted on the Labcorp website, it violated her

rights under CIPA. These third parties obtained this information because Labcorp embedded and configured the Third-party Trackers' software code on its website to surreptitiously track and disclose communications between Ms. Hernandez and Labcorp.

93. Meta, Google, and other third-parties intercepted Ms. Hernandez's private information in California when Labcorp embedded and configured their software code on its website for the purpose of collecting private information from users such as Ms. Hernandez routed that information to third parties through Ms. Hernandez's browser.

94. Ms. Hernandez never consented to the interception of this private information or Labcorp's facilitation of the same.

95. Plaintiff Reynolds is a Pennsylvania resident who visited the Labcorp website (<https://www.labcorp.com/>) beginning in May 2021 and continuing through February 2023 to conduct searches on the website regarding a variety of sensitive medical issues.

96. Ms. Reynolds conducted these searches on the Labcorp website from a web browser while in Pennsylvania.

97. Ms. Reynolds has had a Facebook and/or Meta account, as well as Google account, since approximately 2007.

98. Each time Meta, Google, and other third parties obtained Ms. Reynolds' identifying information and the searches she conducted on the Labcorp website, it violated her rights under CIPA. These third parties obtained this information because Labcorp embedded and configured their software code on its website to surreptitiously track and disclose communications between Ms. Reynolds and Labcorp.

99. Meta, Google, and other third-parties intercepted Ms. Reynolds' private information in California when Labcorp embedded and configured the third parties' software

code on its website for the purpose of collecting private information from users such as Ms. Reynolds routed that information to third parties through Ms. Reynolds' browser.

100. Ms. Reynolds never consented to the interception of this private information or Labcorp's facilitation of the same.

CLASS ACTION ALLEGATIONS

101. Plaintiffs bring this lawsuit under Rules 23(a) and (b) of the Federal Rules of Civil Procedure on behalf of the following Classes:

California Class. All persons in California who entered search terms into Labcorp's website during the time Third-party trackers have been active on Labcorp's website.

Pennsylvania Class. All persons in Pennsylvania who entered search terms into Labcorp's website during the time Third-party trackers have been active on Labcorp's website.

102. Excluded from the Classes are Defendants, any controlled person of Defendants, as well as the officers and directors of Defendants and the immediate family members of any such person. Also excluded are any judge who may preside over this cause of action and the immediate family members of any such person. Plaintiffs reserve the right to modify, change, or expand the Class definitions based upon discovery and further investigation.

103. **Numerosity.** The Classes consist of at least hundreds of individuals, making joinder impractical.

104. **Commonality and Predominance.** Common questions of law and fact exist with regard to the claim and predominate over questions affecting only individual Class members.

Questions common to the Classes include:

- a. Whether Labcorp facilitated or procured the unlawful actions of third parties, including Meta and Google;
- b. Whether Labcorp obtained express consent to their conduct;

c. Whether the conduct of Labcorp violated the California Invasion of Privacy Act, Cal. Penal Code § 631; and

d. Whether the conduct of Labcorp violated the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. § 5701, et seq.;

105. **Typicality.** Plaintiffs' claims are typical of the claims of the Class members in that Plaintiffs, like all Class members, have been injured by Labcorp's misconduct facilitating or procuring third parties to obtain consumers' personal information.

106. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of the Classes. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions, including privacy-protection cases. Plaintiffs do not have any interests antagonistic to those of the Classes.

107. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class-wide damages are essential to induce Labcorp to comply with the law. Moreover, because the amount of each individual Class member's claim is small relative to the complexity of litigation, and because of Labcorp's financial resources, Class members are unlikely to pursue legal redress individually for the violations detailed in this complaint. A class action will allow these claims to be heard where they would otherwise go unheard because of the expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale, and comprehensive supervision by a single court.

108. **Injunctive Relief.** Plaintiffs also satisfy the requirements for maintaining a class under Rule 23(b)(2). Defendants acted on grounds that apply generally to the proposed Classes, making final declaratory or injunctive relief appropriate with respect to the proposed Classes as a whole.

109. **Particular Issues.** Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(c)(4). Their claims consist of particular issues that are common to all Class members and are capable of class-wide resolution that will significantly advance the litigation.

FIRST CAUSE OF ACTION
California Invasion of Privacy Act
Cal. Penal Code §§ 630-638
On Behalf of the California Class Against All Defendants

110. Plaintiffs incorporate and reallege the above factual allegations set forth in paragraph 1 through 109 by reference.

111. Plaintiffs Howard and Hernandez (for the purposes of this section, “Plaintiffs”) bring this Count individually and on behalf of the members of the California Class.

112. The California Invasion of Privacy Act is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose: “The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.”

113. Cal. Penal Code § 631(a) provides that: “Any person who, by means of any machine, instrument, or contrivance, or in any other manner...willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to 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 who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who 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, is punishable by a fine not exceeding two thousand five hundred dollars (\$2,500).”

114. At all relevant times, Meta, Google, and other third parties tracked and intercepted Plaintiffs’ and California Class members’ internet communications exchanged with Labcorp through the Labcorp website.

115. Meta, Google, and other third parties intercepted these communications without consent from all parties to the communications.

116. Meta, Google, and other third parties intended to learn, and did learn, some meaning of the content in the communications including without limitation in the URLs, search queries, and other content described herein exchanged between California Class members and Labcorp on the Labcorp website.

117. The following items constitute “machine[s], instrument[s], or contrivance[s]” under CIPA, and even if they do not, the Meta Pixel, Google Source Code, and source code of the other Third-Party Trackers falls under the broad catch-all category of “any other manner”:

a. The computer codes and programs Meta, Google, and other third parties use and used to track Plaintiffs’ and the California Class members’ communications while they were navigating the Labcorp website and that Labcorp embedded and configured on the Labcorp website;

b. The Plaintiffs’ and California Class members’ browsers, as well as their computing and mobile devices;

c. The web and ad servers from which Meta, Google, and other third parties tracked and intercepted the Plaintiffs' and California Class members' communications while they were using a web browser to access or navigate the Labcorp website;

d. Interception of the Plaintiffs' and California Class members' communications while they were using a browser to visit the Labcorp website.

118. The plan Meta, Google, and other third parties carried out – as facilitated by Labcorp – to effectuate the tracking and interception of the Plaintiffs' and California Class members' communications while they were using a web browser or mobile application to visit Labcorp's website originated in and was executed in California.

119. To facilitate this interception, Labcorp knowingly embedded and configured the Meta Pixel, Google Source Code, and other tracking code developed by third parties on its website, voluntarily selecting settings that increased the amount of information provided to third parties regarding the visitors to Labcorp's website.

120. Labcorp aided and conspired with Meta, Google, and other third parties in allowing them to intercept Plaintiffs' and California Class members' communications with Labcorp by implementing and configuring the Pixel, Google source code, and other third party source code on its website for the purpose of intercepting Plaintiffs' and California Class members' communications with Labcorp.

121. Plaintiffs and California Class members have suffered loss by Labcorp's violations, including by the violation of Cal. Penal Code § 631, and pursuant to Cal. Penal Code § 637.2, Plaintiffs and California Class members seek damages for the greater of \$5,000 per violation or three times the actual amount of damages, as well as injunctive relief.

SECOND CAUSE OF ACTION
Pennsylvania Wiretapping and Electronic Surveillance Control Act

18 Pa. Cons. Stat. § 5701, et seq.
On Behalf of the Pennsylvania Class Against All Defendants

122. Plaintiffs incorporate and reallege the above factual allegations set forth in paragraph 1 through 109 by reference.

123. Plaintiff Deborah Reynolds brings this Count individually and on behalf of the members of the Pennsylvania Class.

124. The Pennsylvania Wiretapping Act prohibits: (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

125. 18 Pa. Cons. Stat. § 5725(a) provides that “[a]ny person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at a rate of \$100 per day for each violation or \$1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys’ fees and other litigation costs incurred.”

126. Reynolds and Pennsylvania Class members engaged in communications with Labcorp through use of Labcorp’s website.

127. Reynolds and Pennsylvania Class members had a justified expectation under the circumstances that their electronic communications would not be intercepted.

128. At all relevant times, Labcorp procured Meta, Google, and other third parties to automatically and secretly intercept Reynolds' and Pennsylvania Class members' internet communications exchanged with Labcorp through the Labcorp website in real-time.

129. To facilitate this interception, Labcorp knowingly embedded and configured the Meta Pixel, Google Source Code, and other tracking code developed by third parties on its website, voluntarily selecting settings that increased the amount of information provided to third parties regarding the visitors to Labcorp's website.

130. Those trackers allowed Meta, Google, and other third parties to intentionally intercept communications in Pennsylvania without consent from all parties to the communications.

131. As a result, Meta, Google, and other third parties intended to learn, and did learn, the content in the communications including without limitation in the URLs, search queries, and other content exchanged between Pennsylvania Class members and Labcorp on the Labcorp website.

132. Reynolds and members of the Pennsylvania Class were not aware that their electronic communications were being intercepted by third parties.

133. The plan to effectuate this tracking and interception of the Plaintiffs' and Pennsylvania Class members' communications while they were using a web browser or mobile application to visit Labcorp's website was executed in Pennsylvania.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, respectfully requests that the Court:

134. Certify this case as a class action, and appoint Plaintiffs as Class Representatives and the undersigned attorneys as Class Counsel;

135. Enter judgment in favor of Plaintiffs and the Classes;
136. Enjoin Labcorp from procuring or facilitating third parties from obtaining Plaintiffs' and Class members' personal information from Labcorp;
137. Award Plaintiffs and Class members statutory damages they are entitled to under CIPA and WESCA;
138. Award Plaintiffs and Class members pre- and post-judgment interest as provided by law;
139. Award Plaintiffs and Class members reasonable litigation expenses and attorneys' fees as permitted by law;
140. Award such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demands a trial by jury of all issues triable as of right.

Dated: September 13, 2023

Respectfully submitted,

/s/ Douglas I Cuthbertson

Douglas I. Cuthbertson*
dcuthbertson@lchb.com
Margaret J. Mattes*
mmattes@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, NY 10013
Telephone: 212.355.9500

Michael W. Sobol*
msobol@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000

Daniel C. Lyon (State Bar No. 43828)
dlyon@emplawfirm.com
ELLIOT MORGAN PARSONAGE
300 E. Kingston Avenue, Suite 200
Charlotte, NC 28203

Telephone: 704.707.3705

Brian Levin*
brian@levinlawpa.com
Kathryn J. Johnson*
kaki@levinlawpa.com
LEVIN LAW, P.A.
2665 South Bayshore Drive, PH2B
Miami, Florida 33133
Telephone: 305.539.0593

Matthew R. Wilson*
mwilson@meyerwilson.com
Michael J. Boyle*
mboyle@meyerwilson.com
MEYER WILSON, P.A.
305 W. Nationwide Blvd
Columbus, Ohio 43215
Telephone: 614.224.6000

*admitted pursuant to LR83.1(d)

Counsel for Plaintiffs and the Proposed Classes

CERTIFICATE OF SERVICE

I, Douglas I. Cuthbertson, certify that on September 13, 2023, I caused the foregoing document to be served on all counsel for all parties to this action by filing it through the Court's ECF system.

DATED September 13, 2023

By: /s/ Douglas I. Cuthbertson
Douglas I. Cuthbertson