UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF CALIFORNIA
CIVIL DIVISION

E.H. and **V.P.**, on behalf of themselves and all others similarly situated, Plaintiffs, v. **LIFELONG ADOPTIONS, INC.**, Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs E.H. and V.P. ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against LifeLong Adoptions, Inc. ("LifeLong" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs' counsel and review of public documents, as to all other matters:

I. INTRODUCTION

1. The decision to place a child up for adoption is one of the most difficult decisions that a woman can make. Moreover, a significant social stigma is often attached to both unplanned pregnancy and placing a child up for adoption. As a result, the unwanted disclosure of such information can be enormously harmful. It can impact an individual's reputation, livelihood, and personal relationships. Thus, if people struggling with the heartbreaking decision of whether to surrender their child to an adoption service are unable to trust that the organizations purporting to offer assistance will protect their sensitive, private information, they are much less likely to seek help when they need it most.

2. Unfortunately, unbeknownst to Plaintiffs and other visitors to Defendant's website, Defendant does not keep sensitive information about its visitors private. Instead, Defendant records the fact that its website visitors, like Plaintiffs and Class Members, are seeking to place their child up for adoption (collectively, "Sensitive Information"), and transmits that information to third party advertisers, including Alphabet, Inc. ("Google") and Meta Platforms, Inc. ("Facebook"), through its use of surreptitious online tracking tools.

3. Online advertising giants, like Google and Facebook, compile as much information as possible about American consumers, including information relating to the most private aspects of their lives, as fuel for their massive, targeted advertising enterprise. As such, any information about a person captured by those online behemoths can be used to stream ads to that person. For example, if Google or Facebook learns that a person is experiencing an unplanned pregnancy, they will use that information to target ads to that person's computers and smartphones for products and services related to pregnancy, adoption, or even abortion services.

4. Google and Facebook offer website operators access to their proprietary suites of marketing, advertising, and customer analytics software, including Google Analytics, Google AdSense, Google Tag Manager, Meta Business Suite, and Facebook Ads (collectively, the "Business Tools"). Armed with these Business Tools, website operators can leverage Google and Facebook's enormous database of consumer information for the purposes of deploying targeted advertisements, performing minute analyses of their customer bases, and identifying new market segments that may be exploited.

5. But, in exchange for access to these Business Tools, website operators install Google and Facebook's surveillance software on their website (the "Tracking Tools"), including 'tracking pixels' ("Pixels") and third-party 'cookies' that capture sensitive, personally identifiable

information provided to the website operator by its website users. This sensitive information can include a unique identifier that Google and Facebook use to identify that user, regardless of what computer or phone is used to access the website. With this unique identifier, Google and Facebook know the identity of the website user, even if that user has never logged into the website they are visiting, or even provided the website with any information about themselves. The Tracking Tools can also capture and share other information like the specific webpages visited by a website user, items added to an online shopping cart by a website user, information entered into an online form by a website user, and the device characteristics of a website user's phone or computer. This means that simply browsing a web page that has the Tracking Tools on it creates a beacon that Google, Facebook, and their clients can use to track that person's use of the website.

6. In essence, when website operators use Google and Facebook's Business Tools, they choose to participate in Google and Facebook's mass surveillance network and, in turn, benefit from Google and Facebook's collection of user data at the expense of their customers' privacy.

7. LifeLong is one of the many organizations that has chosen to prioritize its marketing efforts over its customers' privacy, by installing Google and Facebook's Tracking Tools on its website.

8. LifeLong is an adoption clinic that serves families looking to adopt, and looking to put a child up for adoption, throughout the United States.[1] LifeLong's website – www.lifelongadoptions.com/ (the "Website") – specifically targets pregnant women, and urges them to contact LifeLong for a consultation regarding placing their child for adoption by filling

[1] *Home* Page, LIFELONG ADOPTIONS, https://www.lifelongadoptions.com/ (last visited Mar. 26, 2025).

out an online form, or launching a phone call directly through the Website.[2] The Website also allows pregnant mothers to download informational material specifically written for mothers considering placing a child up for adoption, take a "Birthmother Communication Quiz" to identify the type of adoption that would be best for their circumstances, and even review potential families that are looking to adopt a child.[3]

9. Plaintiffs and Class Members visited the Website and had their personal Sensitive Information tracked by Defendant using the Tracking Tools. However, Defendant ***never*** informed Plaintiffs or Class Members that they were being tracked, never obtained authorization from Plaintiffs or Class Members to share their Sensitive Information with third parties, and never obtained Plaintiffs and Class Members informed consent for such Sensitive Information to be transmitted to the third parties. Nevertheless, through the Tracking Tools, Defendant intentionally and willfully shared the Sensitive Information with Google, the largest advertiser and compiler of user information, or Facebook, the largest social media company on earth, both of which have a sordid history of privacy violations in pursuit of ever-increasing advertising revenue.[4]

10. As a result of Defendant's conduct, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lack of trust in communicating with

[2] *See, e.g.*, *Why Consider Adoption*, LIFELONG ADOPTIONS, https://www.lifelongadoptions.com/pregnant/why-consider-adoption (last accessed Mar. 26, 2025); *Benefits of Adoption*, LIFELONG ADOPTIONS, https://www.lifelongadoptions.com/benefits-of-adoption (last accessed Mar. 26, 2025).

[3] *See Find Adoptive Families*, LIFELONG ADOPTIONS, https://www.lifelongadoptions.com/family-finder-lp (last accessed Mar. 26, 2025); *Birthmoter Communication Quiz*, LIFELONG ADOPTIONS, https://www.lifelongadoptions.com/communication-quiz-lp (last accessed Mar. 26, 2025).

[4] This Court will not have to look far to find evidence of Meta's violations of privacy laws. Just in May of this year the European Union fined Meta "a record-breaking" $1.3 billion for violating EU privacy laws. *See* Hanna Ziady, *Meta slapped with record $1.3 billion EU fine over data privacy*, https://www.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html (last visited Mar. 26, 2025).

online service providers; (iii) emotional distress and heightened concerns related to the release of Sensitive Information to third parties, (iv) loss of benefit of the bargain; (v) diminution of value of the Sensitive Information; (vi) statutory damages and (viii) continued and ongoing risk to their Sensitive Information.

11. Therefore, Plaintiffs seek, on behalf of themselves and a class of similarly situated persons, to remedy these harms and assert the following statutory and common law claims against Defendant: Invasion of Privacy; Breach of Confidence; Breach of Fiduciary Duty; Negligence; Breach of Implied Contract; Unjust Enrichment; and violations of the Electronic Communications Privacy Act ("ECPA"), California Unfair Competition Law ("UCL"), Pennsylvania Wiretapping and Electronic Surveillance Control Act ("WESCA"), and Pennsylvania Unfair Trade practice and Consumer Protection Law ("UTPCPL").

II. PARTIES

Plaintiff E.H.

12. Plaintiff E.H. is a citizen of the State of California, residing in Fresno County, and brings this action both in an individual capacity, and on behalf of all others similarly situated.

13. In or around November of 2024, Plaintiff E.H. utilized Defendant's Website on her personal electronic devices to request a consultation due to an unplanned pregnancy, and consequently had her Sensitive Information tracked and disclosed, in the same manner as depicted in Sec. IV(A)(d), *infra*.

14. Plaintiff E.H. never authorized Defendant to disclose any aspect of these very personal communications with Defendant through its Website to third parties, including the Sensitive Information that she provided to Defendant.

15. On every occasion that she visited Defendant's Website, Plaintiff E.H. possessed accounts with Google and Facebook, and she accessed Defendant's Website while logged into her

Google and Facebook accounts on the same device. E.H. did not know that by being logged in when she visited Defendant's Website, Defendant would allow Google and Facebook to track her every move.

16. After providing her Sensitive Information to Defendant through the Website, Plaintiff E.H. immediately began seeing targeted online advertisements for adoption services, further confirming that her Sensitive Information had been shared with unauthorized third parties.

Plaintiff V.P.

17. Plaintiff V.P. is a citizen of the State of Pennsylvania, residing in Crawford County, and brings this action both in an individual capacity, and on behalf of all others similarly situated.

18. In or around May of 2022, Plaintiff V.P. utilized Defendant's Website on her personal electronic devices to request a consultation due to an unplanned pregnancy, and consequently had her Sensitive Information tracked and disclosed, in the same manner as depicted in Sec. IV(A)(d), *infra*.

19. Plaintiff V.P. never authorized Defendant to disclose any aspect of these very personal communications with Defendant through its Website to third parties, including the Sensitive Information that she provided to Defendant.

20. On every occasion that she visited Defendant's Website, Plaintiff V.P. possessed accounts with Google and Facebook, and she accessed Defendant's Website while logged into her Google and Facebook accounts on the same device. V.P. did not know that by being logged in when she visited Defendant's Website, Defendant would allow Google and Facebook to track her every move.

21. After providing her Sensitive Information to Defendant through the Website, Plaintiff V.P. immediately began seeing targeted online advertisements for adoption services, further confirming that her Sensitive Information had been shared with unauthorized third parties.

Defendant LifeLong Adoptions, Inc.

22. Defendant LifeLong Adoptions, Inc. is a domestic business corporation incorporated in the State of Illinois, with its principal place of business at 820 E. Terra Cotta Avenue, Suite 145, Crystal Lake, IL, in McHenry County.

III. JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members and minimal diversity exists because Plaintiffs and many putative class members are citizens of a different state than Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

24. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges question of federal laws under the ECPA (18 U.S.C. § 2511, *et seq.*).

25. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

26. This Court has personal jurisdiction over Defendant because Defendant has advertised its services to consumers in the State of California and in this judicial district, and Defendant has harmed Class Members in this district, including Plaintiff E.H.

27. Personal jurisdiction is also proper because Defendant committed tortious acts in the State of California and this judicial district and Plaintiffs' claims arise out of such acts, and/or because Defendant has otherwise made or established contacts in the State California and in this

judicial district sufficient to permit the exercise of personal jurisdiction, including by stating that "[a]ny claim relating to Lifelong Adoptions' web site shall be governed by the laws of the State of California without regard to its conflict of law provisions" in the Terms and Conditions of Use posted on its Website when it was accessed by Plaintiffs.[5]

28. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to the claims in this action occurred in this judicial district.

IV. FACTUAL ALLEGATIONS

A. DEFENDANT'S USE OF THIRD-PARTY TRACKING TECHNOLOGIES

a. Google and Facebook's Mass Advertising Surveillance Operation

29. Google is the largest digital advertiser in the country, accounting for 26.8-percent of the total digital advertising revenue generated in the United States.[6] In 2023, Google's advertising revenue of $238 billion accounted for 77-percent of its total revenue for the year.[7]

30. Google advertises Google Analytics and other Business Tools to website operators, like Defendant, claiming they will allow the operator to "[u]nderstand [their] site and app users," "check the performance of [their] marketing," and "[g]et insights only Google can give."[8] But, in

---

[5] *See Lifelong Adoptions Terms of Use*, LIFELONG ADOPTIONS, (www.lifelongadoptions.com/terms : July 2, 2022), *archived at*: WAYBACK MACHINE, web.archive.org/web/20220702170340/https://www.lifelongadoptions.com/terms (last accessed Mar. 28, 2025).

[6] *Share of major ad-selling companies in digital advertising revenue in the United States*, STATISTA (May 2024), https://www.statista.com/statistics/242549/digital-ad-market-share-of-major-ad-selling-companies-in-the-us-by-revenue/#:~:text=In%202023%2C%20Google%20accounted%20for,21.1%20and%2012.5%20percent%2C%20respectively https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/ (last visited Mar. 26, 2025).

[7] Florian Zandt, *Google's Ad Revenue Dwarfs Competitors*, STATISTA (Sep. 10, 2024), https://www.statista.com/chart/33017/annual-advertising-revenue-of-selected-tech-companies-offering-search-solutions/#:~:text=Online%20advertising&text=Alphabet%2C%20the%20company%20behind%20the,overall%20revenue%20this%20past%20year (last visited Mar. 26, 2025).

[8] *Welcome to Google Analytics*, GOOGLE, https://analytics.google.com/analytics/web/provision/?authuser=0#/provision (last visited Mar. 26, 2025).

order for website operators to get information from Google Analytics about their website's visitors, they must allow data collection through installation of Google's Tracking Tools on their website.[9]

31. Indeed, on its *Privacy & Terms* page, Google admits that it collects information from third party websites, stating that: "[m]any websites and apps use Google services to improve their content and keep it free. When they integrate our services, these sites and apps share information with Google."[10]

32. Google also admits that it uses the information collected from third party websites, such as Defendant's, to sell targeted advertising, explaining to users that: "[f]or example, a website that sells mountain bikes might use Google's ad services. After you visit that site, you could see an ad for mountain bikes on a different site that shows ads served by Google."[11]

33. Facebook operates the world's largest social media company, and the vast majority of its revenue comes from selling advertising space on its platform. In 2021, Facebook generated $117 billion, roughly 97% of which was derived from the sale of digital advertisements.[12]

34. Facebook markets its Business Tools to website operators, claiming that that its Business Tools can:

> [H]elp website owners and publishers, app developers, and business partners, including advertisers and others, integrate and share data with Meta, understand

[9] *See* Aaron Ankin & Surya Matta, *The High Privacy Cost of a "Free" Website*, THE MARKUP, https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites (last visited Mar. 26, 2025).

[10] *Privacy & Terms – How Google uses information from sites or apps that use our services*, GOOGLE, https://policies.google.com/technologies/partner-sites (last visited Mar. 26, 2025).

[11] *Id*.

[12] *Meta Reports Fourth Quarter and Full Year 2021 Results*, META, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Mar. 26, 2025).

> and measure their products and services, and better reach and serve people who use or might be interested in their products and services.[13]

35. But, like with Google, website operators using Facebook's Business Tools must install Facebook's Tracking Tools on their website. Facebook readily admits that it "receives information from [third-party] businesses and organizations," such as Defendant, and uses that information to sell targeted advertising.[14] By way of example, Facebook's online *Help Center* explains that users "may see [Facebook] ads for hotel deals if [they] visit travel websites."[15]

36. While Google and Facebook admit that they collect information from third-party websites through the Tracking Tools, neither provides, nor could provide, a publicly available list of every webpage on which their Tracking Tools are installed. As such, the vague descriptions of Google and Facebook's data collection practices referenced above could not give Plaintiffs and Class Members any reason to think that Defendant was part of Google and Facebook's surveillance network. Moreover, as Defendant does not disclose its use of Google and Facebook's Tracking Tools, Plaintiffs and Class Members could not have been reasonably expected to review any of Google and Facebook's privacy statements in connection with their use of the Website

37. Google and Facebook aggregate the user information that they collect from third-party websites into "advertising profiles" consisting of all of the data that they have collected about a given user.[16] With these advertising profiles, Google and Facebook can sell hyper-precise

---

[13] *The Meta Business Tools*, FACEBOOK HELP CENTER, https://www.facebook.com/help/331509497253087?helpref=faq_content (last visited Mar. 26, 2025).

[14] *How Meta receives information from other business and organizations*, FACEBOOK HELP CENTER, https://www.facebook.com/help/2230503797265156/?helpref=related_articles (last visited Mar. 26, 2025).

[15] *Id*.

[16] Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*, ELECTRONIC FRONTIER FOUNDATION (2019), *available online at*: https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance_0.pdf.

advertising services, allowing their clients to target internet users based on combinations of their location, age, race, interests, hobbies, life events (e.g., recent marriages, graduation, or relocation), political affiliation, education level, home ownership status, marital status, household income, type of employment, use of specific apps or websites, and more.[17]

38. Google and Facebook's surveillance of individual's internet usage is ubiquitous. In 2017, Scientific American reported that over 70-percent of smartphone apps report "personal data to third-party tracking companies like Google[, and] Facebook[.]"[18] Google trackers are present on 74-percent of all web traffic, and 16-percent of websites have a hidden Facebook tracking Pixel.[19]

39. Moreover, as in this case, the data collected by Google and Facebook often pertains to the most personal and sensitive aspects of an individual's life. For example:

a. 93-percent of pornography websites allow third parties, including Google and Facebook, to collect their user's browsing habits.[20] In fact, Google advertising trackers were found on 73-percent of pornography websites.[21]

[17] *About audience segments*, GOOGLE ADS, https://support.google.com/google-ads/answer/2497941?hl=en#zippy=%2Cin-market-segments%2Caffinity-segments%2Clife-events%2Cdetailed-demographics (last visited Mar. 26, 2025); *Facebook Ads: Who You Can Target*, SEOM Interactive, https://searchenginesmarketer.com/company/resources/facebook-ads-can-target/ (last visited Mar. 26, 2025).

[18] Narseo Vallina-Rodriguez & Srikanth Sundaresan, *7 in 10 Smartphone Apps Share Your Data with Third-Party Services*, SCIENTIFIC AMERICAN (May 30, 2017), https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/ (last visited Mar. 26, 2025).

[19] *WhoTracksMe*, Ghostery, https://www.ghostery.com/whotracksme/ (last visited Mar. 26, 2025).

[20] Elena Maris, Timothy Libert & Jennifer R. Henrichsen, *Tracking sex: The implications of widespread sexual data leakage and tracking on porn websites*, NEW MEDIA & SOCIETY (2020), *available online at*: https://journals.sagepub.com/doi/10.1177/1461444820924632.

[21] *Id*.

b. 81-percent of the most popular mobile apps for managing depression and quitting smoking allowed Facebook and/or Google to access subscriber information, including health diary entries and self-reports about substance abuse.[22]

c. Twelve of the largest pharmacy providers in the United States send information regarding user's purchases of products such as pregnancy tests, HIV tests, prenatal vitamins, and Plan B to online advertisers.[23] For example, when an online shopper searches for a pregnancy test, views the product page for a pregnancy test, or adds a pregnancy test to their online shopping cart on Kroger's website, that information is transmitted to Google and Facebook.[24]

d. Thirty-three of the most popular crisis center websites provide information to Facebook through its Meta Pixel, including, in some cases, that users filled out a contact form or clicked a button to initiate a call to a suicide helpline.[25]

40. This monumental, invasive surveillance of Americans' internet usage is not accidental. As Google's then-CEO Eric Schmit admitted in 2010: "We know where you are. We know where you've been. We can more or less know what you're thinking about."[26] Likewise, in 2008, Facebook CEO Mark Zuckerberg predicted that the amount of information shared by

[22] Kit Huckvale, John Torous & Mark E. Larsen, *Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation*, JAMA NETWORK OPEN (2019), *available online at*: https://pubmed.ncbi.nlm.nih.gov/31002321/.

[23] Darius Tahir & Simon Fondrie-Teitler, *Need to Get Plan B or an HIV Test Online? Facebook May Know About It*, THE MARKUP (June 30, 2023), https://themarkup.org/pixel-hunt/2023/06/30/need-to-get-plan-b-or-an-hiv-test-online-facebook-may-know-about-it (last visited Mar. 26, 2025).

[24] Jon Keegan, *Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You*, THE MARKUP (Feb. 16, 2023), https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you (last visited Mar. 26, 2025).

[25] Colin Lechner & Jon Keegan, *Suicide Hotlines Promise Anonymity. Dozens of Their Websites Send Sensitive Data to Facebook*, THE MARKUP (June 30, 2023), https://themarkup.org/pixel-hunt/2023/06/13/suicide-hotlines-promise-anonymity-dozens-of-their-websites-send-sensitive-data-to-facebook (last visited Mar. 26, 2025).

[26] Andrew Orlowski, *Google's Schmidt: We know what you're thinking*, THE REGISTER (Oct. 4, 2020), https://www.theregister.com/2010/10/04/google_ericisms/ (last visited Mar. 26, 2025).

individuals online will likely double every year, and Facebook's best strategy is to be "pushing that forward."[27]

41. In fact, Google and Facebook value user information so highly that they provide their Business Tools to many website operators for free, all to expand their surveillance apparatus.[28]

42. When website operators, like Defendant, make use of Google and Facebook's Business Tools, they are essentially choosing to participate in Google and Facebook's mass surveillance network, and in return they benefit from Google and Facebook's collection of user data, at the expense of their website users' privacy. For example, in exchange for allowing it to collect user information, Facebook allows website operators to target customers with "dynamic advertisements" personalized to individual consumers using the user information that Facebook collects from all across the internet.[29] Likewise, Google rewards website operators for providing it with their user's information by granting access to its Analytics platform, which leverages demographic data collected by Google to provide detailed analyses of the website's user base.[30]

43. In many cases, a website operator's use of third-party tracking software is not disclosed whatsoever in its privacy policy.[31] Even where the use of such third-party software is

---

[27] Michael Zimmer, *Mark Zuckerberg's Theory of Privacy,* THE WASHINGTON POST (Feb. 4, 2014), https://www.washingtonpost.com/lifestyle/style/mark-zuckerbergs-theory-of-privacy/2014/02/03/2c1d780a-8cea-11e3-95dd-36ff657a4dae_story.html (last visited Mar. 26, 2025).

[28] *Analytics Overview*, GOOGLE, https://marketingplatform.google.com/about/analytics/ (last visited Mar. 26, 2025) ("Google Analytics gives you the tools, free of charge"); *Meta Business Suite FAQ*, META, https://www.facebook.com/business/tools/meta-business-suite/help (last visited Mar. 26, 2025) ("Meta Business Suite is a free tool").

[29] *Retargeting*, META, https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited Mar. 26, 2025).

[30] *Google Marketing Platform – Features*, GOOGLE, https://marketingplatform.google.com/about/analytics/features/ (last visited Mar. 26, 2025).

[31] *See* Woodrow Hartzog, *Privacy's Blueprint*, 60-67 (Harvard University Press 2018) (detailing deficiencies with online privacy policies).

disclosed, such disclosures are often hidden and cloaked in such confusing, technical and overly legal language as to be indecipherable to the typical internet user.[32]

44. Moreover, for even a conscientious internet user, the massive volume of privacy policies encountered through routine internet use makes reviewing each and every one practically impossible. According to one study, it would take the average internet user 244 hours – or 30.5 working days – to read the privacy policy of every new website that they visited in a single year.[33]

b. Pixels Can Record Almost Every Interaction Between a User and a Website

45. In order to use Google and Facebook's Business Tools, Defendant installed Google and Facebook's Tracking Tools, including tracking Pixels, onto its website.

46. Pixels are one of the tools used by website operators to track user behavior. As the Federal Trade Commission ("FTC") explains, a Pixel is:

> [A] small piece of code that will be placed into the website or ad and define [the Pixel operator's] tracking goals such as purchases, clicks, or pageviews…
>
> Pixel tracking can be monetized several ways. One way to monetize pixel tracking is for companies to use the tracking data collected to improve the company's own marketing campaigns…Another is that companies can monetize the data collected by further optimizing their own ad targeting systems and charging other companies to use its advertising offerings.[34]

47. Pixels can collect a shocking amount of information regarding an individual's online behavior, including the webpages viewed by the user, the amount of time spent by the user on specific webpages, the specific buttons and hyperlinks that the user clicks, the items that the

---

[32] *Id*.

[33] Aleecia M. McDonald & Lorrie Faith Cantor, *The Cost of Reading Privacy Policies*, I/S: A JOURNAL OF LAW AND POL. FOR THE INFO. SOC. (2008), *available online at*: https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

[34] *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FEDERAL TRADE COMMISSION – OFFICE OF TECHNOLOGY (Mar. 6, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking (last visited Mar. 26, 2025).

user adds to an online shopping cart, the purchases that a user makes through an online retailer, the text entered by the user into a website search bar, and even the information provided by the user on an online form.[35]

48. But most internet users are completely unaware that substantial information about their internet usage is being collected through tracking Pixels. The FTC warns that:

> Traditional controls such as blocking third party cookies may not entirely prevent pixels from collecting and sharing information. Additionally, many consumers may not realize that tracking pixels exist because they're invisibly embedded within web pages that users might interact with…Academic and public reporting teams have found that thousands of the most visited webpages have pixels and other methods that leak personal information to third parties.[36]

c. The Pixels Installed on Defendant's Website Transmit Personally Identifiable Information to Google and Facebook

49. Every website is hosted by a computer "server" that holds the website's contents.

50. To access a website, individuals use "web browsers." Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the Internet. Each "client device" (such as a computer, tablet, or smartphone) accesses web content through a web browser (such as Google's Chrome, Mozilla's Firefox, Apple's Safari, or Microsoft's Edge).

51. Communications between a website server and web browser consist of Requests and Responses. Any given browsing session may consist of hundreds or even thousands of individual Requests and Responses. A web browser's Request asks the website to provide certain

[35] *See id.*; *How does retargeting on Facebook help your business?*, META, https://www.facebook.com/business/goals/retargeting (last visited Mar. 26, 2025); Tom Kemp, *"Oops! I Did It Again" ... Meta Pixel Still Hoovering Up Our Sensitive Data*, MEDIUM, https://tomkemp00.medium.com/oops-i-did-it-again-meta-pixel-still-hoovering-up-our-sensitive-data-f99c7b779d47#_ftn1 (last visited Mar. 26, 2025).

[36] *Lurking Beneath the Surface, supra* note 34.

information, such as the contents of a given webpage when the user clicks a link, and the Response from the website sends back the requested information – the web pages' images, words, buttons, and other features that the browser shows on the user's screen as they navigate the website.

52. Additionally, on most websites, the Response sent back to the user's web browser directs the browser to create small files known as "cookies" on the user's device.[37] These cookies are saved by the user's web browser, and are used to identify the website user as they browse the website or on subsequent visits to the site.[38] For example, in a more innocuous use case, a cookie may allow the website to remember a user's name and password, language settings, or shopping cart contents.[39]

53. When a Google/Facebook user logs onto their account, their web browser records a Google/Facebook tracking cookie.[40] These cookies include a specific line of code that links the web browser to the user's Google/Facebook account.[41]

54. Google and Facebook's Pixels use cookies, but operate differently than cookies. Rather than directing the browser to save a file on the user's device, the Pixels acquires information from the browser, without notifying the user. The information can include details about the user, his or her interactions with the Website, and information about the user's environment (*e.g.,* type of device, type of browser, and sometimes even the physical location of the device).

[37] *What is a web browser?*, MOZILLA, https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/ (last visited Mar. 26, 2025).

[38] *Id*.

[39] *Id*.

[40] Cyphers, *supra* note 16.

[41] *Id*.

55. Simultaneously, the Google and Facebook Pixels, like those installed on Defendant's Website, request identifying information from any Google and Facebook cookies previously installed on the user's web browser.

56. The Pixel then combines the data it received from the browser with the data it acquired from the cookie, and instructs the web browser to transmit the information back to Google and Facebook. As a result, Google and Facebook can link all of the user information collected by their Pixels on the Defendant's Website to the user's identity, via the user's Google or Facebook profile. Thus, even if a user never actually logs into a website, or fills out a form, the website, along with Google and Facebook, can know the user's identity.

57. A remarkable number of Americans possess a Google or Facebook account. According to a 2023 survey, 68-percent of Americans report that they are users of Facebook.[42] And just one of Google's many products, its Gmail e-mail client, is used by over one-third of Americans.[43] When these users visit a website, like Defendant's, that utilizes a Google or Facebook Pixel, any information collected by the Pixel can be linked to the user's identity through the Google and Facebook cookies installed on the user's web browser.

58. However, it is not only Google and Facebook account holders that are at risk of having Pixel-collected website data linked to their identities. Rather, Google and Facebook utilize sophisticated data tracking methods to identify even those few users who do not have a Google or Facebook account.

---

[42] Katherine Schaeffer, *5 facts about how Americans use Facebook, two decades after its launch*, PEW RESEARCH (Feb. 2, 2024), https://www.pewresearch.org/short-reads/2024/02/02/5-facts-about-how-americans-use-facebook-two-decades-after-its-launch/ (last visited Mar. 26, 2025).

[43] *See* Harsha Kiran, *49 Gmail Statistics To Show How Big It Is In 2024*, TECHJURY (Jan. 3, 2024), https://techjury.net/blog/gmail-statistics/ (last visited Mar. 26, 2025) ("Gmail accounts for 130.9 million of the total email users in the US"). The United States population is approximately 337.4 million. *See* UNITED STATES CENSUS BUREAU, https://www.census.gov/popclock/ (last visited Mar. 26, 2025).

59. Google and Facebook's Pixels, like those on Defendant's website, can acquire information about the user's device and browser, such as their screen resolution, time zone setting, browser software type and version, operating system type and version, language setting, and IP address.

60. An internet user's combination of such device and browser characteristics, commonly referred to as their "browser fingerprint," is "often unique."[44] By tracking this browser fingerprint, Google and Facebook are able to compile a user's activity across the internet.[45] And, as Google and Facebook continuously compile user data over time, their understanding of the user's browser fingerprint becomes more sophisticated such that they need only to collect a single piece of identifying information to identify the user linked to a browser fingerprint.

61. While debating the Video Privacy Protection Act[46] on the Senate floor in 1988, Senator Patrick Leahy remarked:

> [I]n an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone…I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against…
>
> [Privacy] is not a conservative or a liberal or moderate issue. It is an issue that goes to the deepest yearnings of all Americans that we are free and we cherish our freedom and we want our freedom. We want to be left alone.

S. Rep. No. 100-599 at pp. 5-6 (1988).

62. Now, almost forty years later, Senator Leahy's nightmare has become reality. Through the use of Internet surveillance technology, almost every facet of our relationships,

[44] Cyphers, *supra* note 16.

[45] *Id*.

[46] 18 U.S.C. § 2710, *et seq*.

interests, aspirations, and beliefs can be tracked, recorded, and packaged for corporate profit by website operators like Defendant.

63. Through this action, Plaintiffs seek to send Defendant, and other corporations like it, the same message that Senator Leahy elucidated during the Internet's infancy: "[W]e are free and we cherish our freedom and we want our freedom. We want to be left alone." *Id*.

d. Defendant Disclosed Plaintiffs' and Class Members' Sensitive Information to Google and Facebook

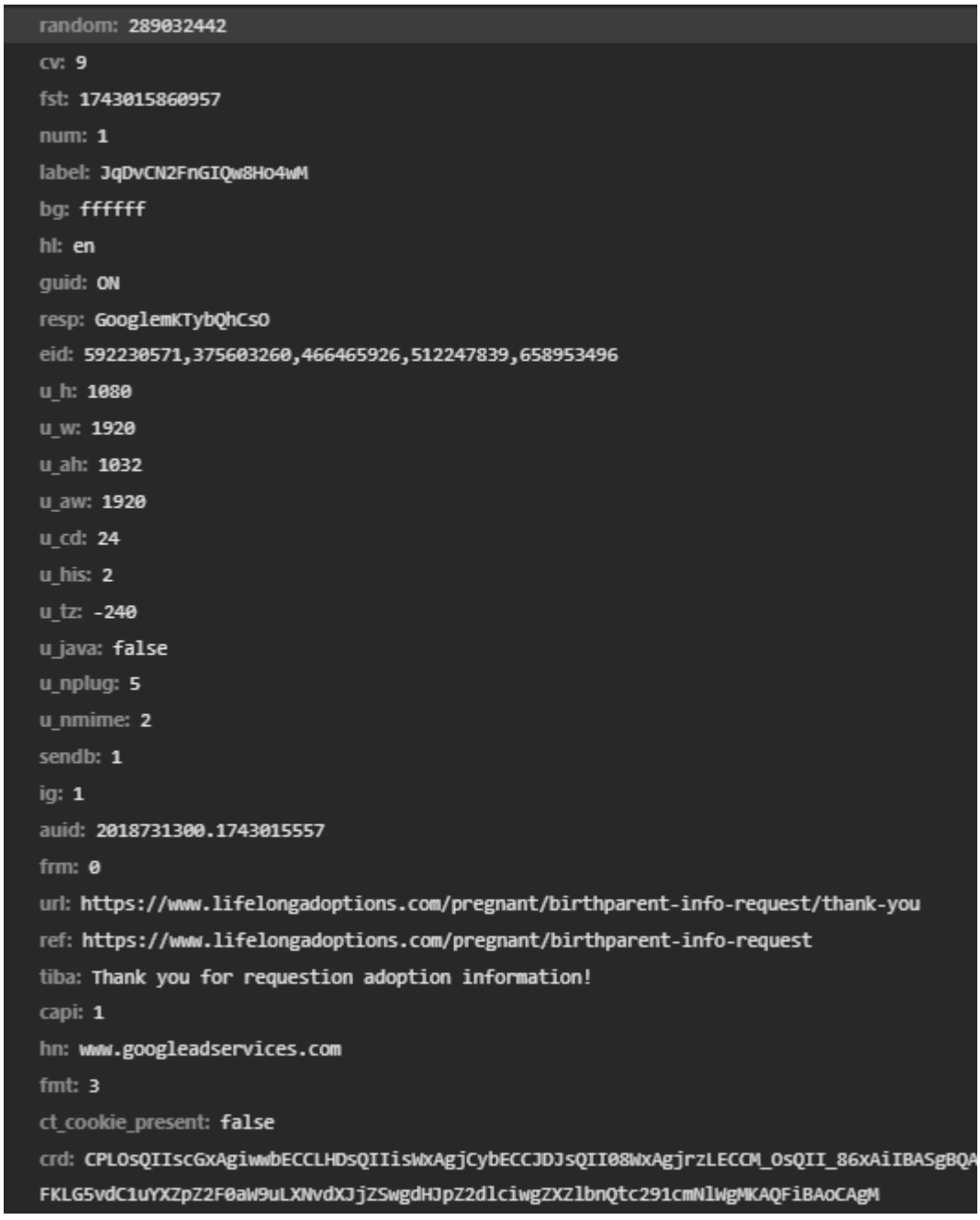
64. Plaintiffs and Class Members all visited the Website to seek Defendant's guidance while considering the immense decision of whether to place their child up for adoption.

65. Unbeknownst to Plaintiffs and Class Members, Defendant intentionally configured the Google and Facebook Pixels installed on its Website to capture and transmit the Sensitive Information that they communicated to Defendant while completing these online forms to unauthorized third parties, including Google and Facebook.

66. For example, the following screenshots ("Figures 1 & 2") depict network transmission data captured from the Website, and shows that when expectant mothers, including Plaintiffs and Class Members, use the contact form on the Website for inquiries regarding placing a child up for adoption, the Tracking Tools installed on the Website transmit the fact that the Website user has visited a page titled "Pregnant & Considering Adoption? Get Info," and has submitted an application to receive further information, to Google and Facebook.

67. Further, the information transmitted to Google and Facebook was accompanied by specific lines of code linking the Sensitive Information provided by Plaintiffs to their identities. The following screenshot shows that the Google Pixel on Defendant's website transmitted the identifier number attached to Google's "_cid" and "_sid" cookies, which identify, and link the user's Website behavior to the user's Google account, along with other information that is

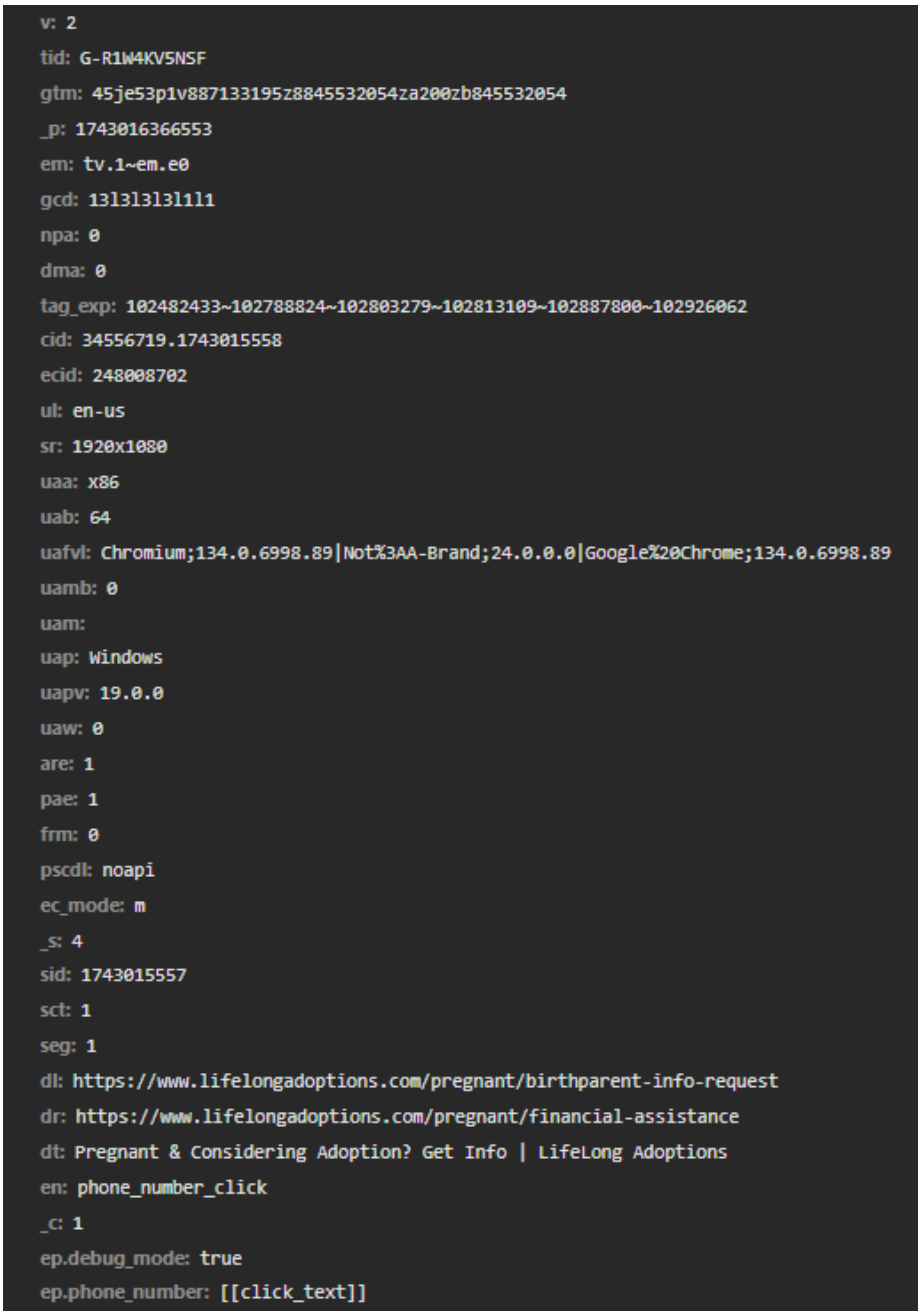
commonly used to create a browser fingerprint, such as the user's language selection, screen resolution, operating system software and version number, and internet browser software and version number. Likewise, the Facebook Pixel on Defendant's Website transmitted the identified number attached to Facebook's "fbp" cookie, which identifies, and links the user's Website behavior to the user's Facebook account.

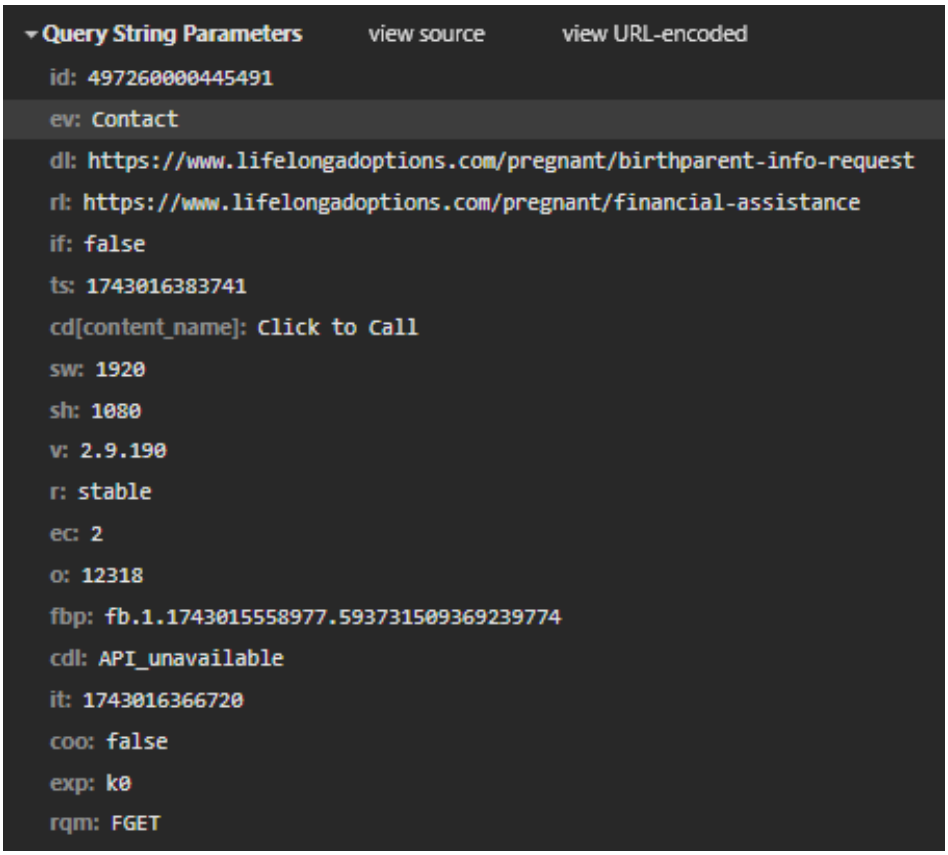


Figures 1 & 2. Screenshots depicting back-end network traffic from Defendant's Website which show the information transmitted to Google and Facebook when Website users submit a request for further information regarding placing a child up for adoption.

68. The Website also informs Facebook and Google when a mother initiates a call to Defendant to seek an adoption consultation. As the screenshots below ("Figures 3 and 4") show, when Website users initiate a call to Defendant from the portion of the Website titled "Pregnant & Considering Adoption? Get Info," the Tracking Technology installed on Defendant's Website transmit the fact that the user initiated a call regarding an unplanned pregnancy to Google and

Facebook, alongside the identifier number attached to Google's "_cid" and "_sid" cookies and Facebook's "fbp" cookie, which identify, and link the user's Website behavior to the user's Google and Facebook accounts, as well as other information that is commonly used to create a browser fingerprint, such as the user's language selection, screen resolution, operating system software and version number, and internet browser software and version number.

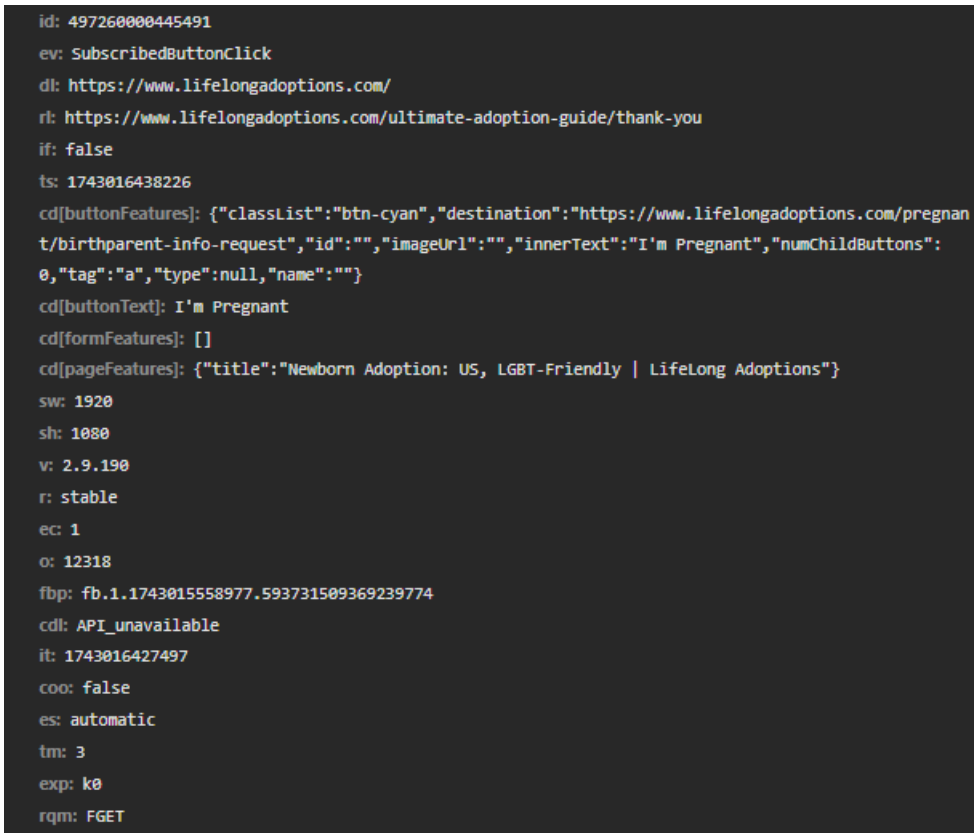




Figures 3 & 4. Screenshots depicting back-end network traffic from Defendant's Website which shows information transmitted to Google and Facebook when Website users initiate a call to request information regarding placing a child up for adoption.

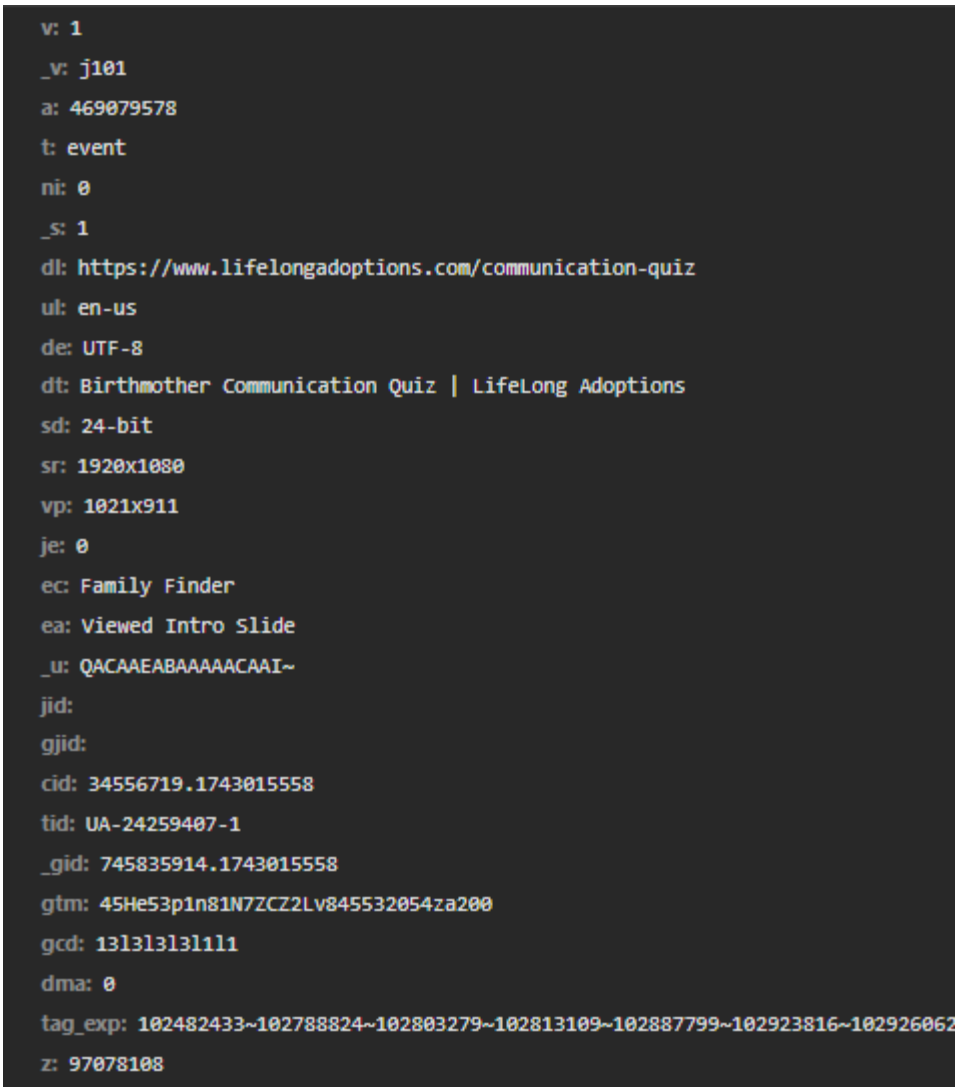
69. But, Defendant's use of the Tracking Technology is not just limited to its contact tools. As the screenshots below (Figures 5 & 6) show, when a Website user downloads Defendant's "Ultimate Adoption Guide," the Tracking Technologies notify Google and Facebook that the Website user has downloaded the "Ultimate Adoption Guide" by clicking the button labeled "I'm Pregnant," transmitted alongside the identifier number attached to Google's "_cid" and "_sid" cookies and Facebook's "fbp" cookie, which identify, and link the user's Website behavior to the user's Google and Facebook accounts, as well as other information that is commonly used to create a browser fingerprint, such as the user's language selection, screen resolution, operating system software and version number, and internet browser software and version number.

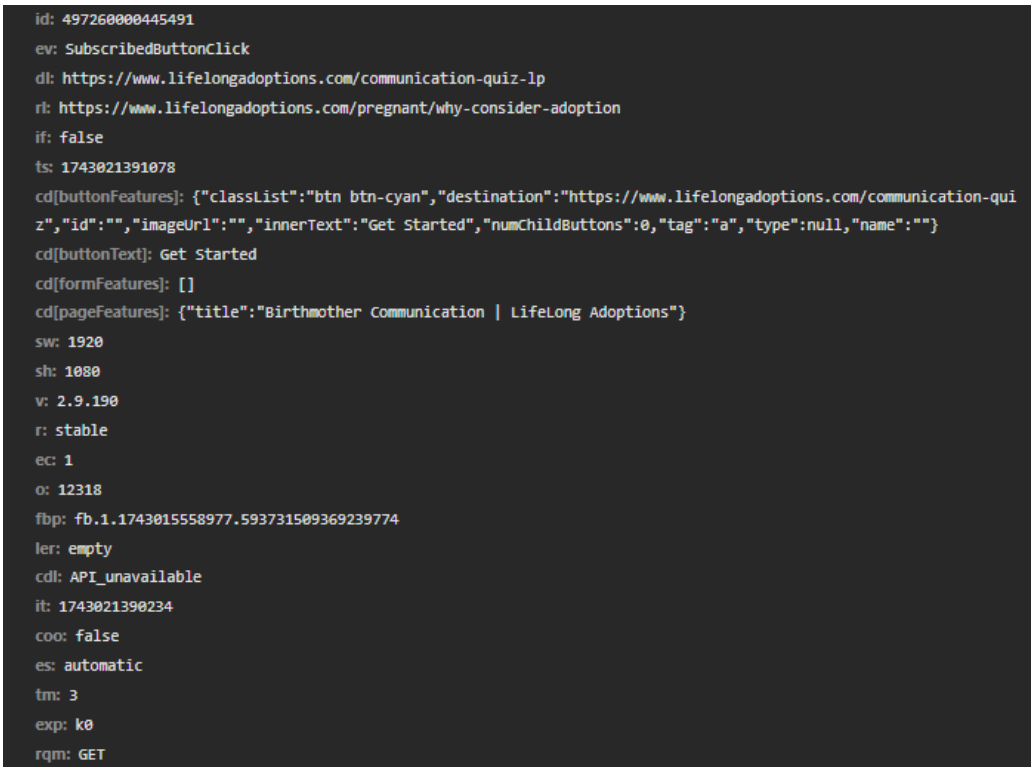
```
v: 2
tid: G-R1W4KV5NSF
gtm: 45je53p1v887133195z8845532054za200zb845532054
_p: 1743016427154
gcd: 13l3l3l3l1l1
npa: 0
dma: 0
tag_exp: 102482433~102788824~102803279~102813109~102887800~102926062
cid: 34556719.1743015558
ecid: 248008702
ul: en-us
sr: 1920x1080
uaa: x86
uab: 64
uafvl: Chromium;134.0.6998.89|Not%3AA-Brand;24.0.0.0|Google%20Chrome;134.0.6998.89
uamb: 0
uam:
uap: Windows
uapv: 19.0.0
uaw: 0
are: 1
pae: 1
frm: 0
pscdl: noapi
_s: 3
sid: 1743015557
sct: 1
seg: 1
dl: https://www.lifelongadoptions.com/
dr: https://www.lifelongadoptions.com/ultimate-adoption-guide/thank-you
dt: Newborn Adoption: US, LGBT-Friendly | LifeLong Adoptions
en: im_pregnant_click
ep.debug_mode: true
_et: 6937
tfd: 11951
```



Figures 5 & 6. Screenshots depicting back-end network traffic from Defendant's Website which shows information transmitted to Google and Facebook when Website users download the "Ultimate Adoption Guide."

70. Defendant's Website also notifies Google and Facebook when the Website user takes Defendant's "Birthmother Communication Quiz." As the screenshots below (Figures 7 & 8) show, when a Website user accesses the "Birthmother Communication Quiz," the Tracking Technology notifies Google and Facebook that the quiz has been taken by transmitting either that the user "viewed the intro slide" or clicked the "get started" button, alongside the identifier number attached to Google's "_cid" and "_sid" cookies and Facebook's "fbp" cookie, which identify, and link the user's Website behavior to the user's Google and Facebook accounts, as well as other information that is commonly used to create a browser fingerprint, such as the user's language selection, screen resolution, operating system software and version number, and internet browser software and version number.

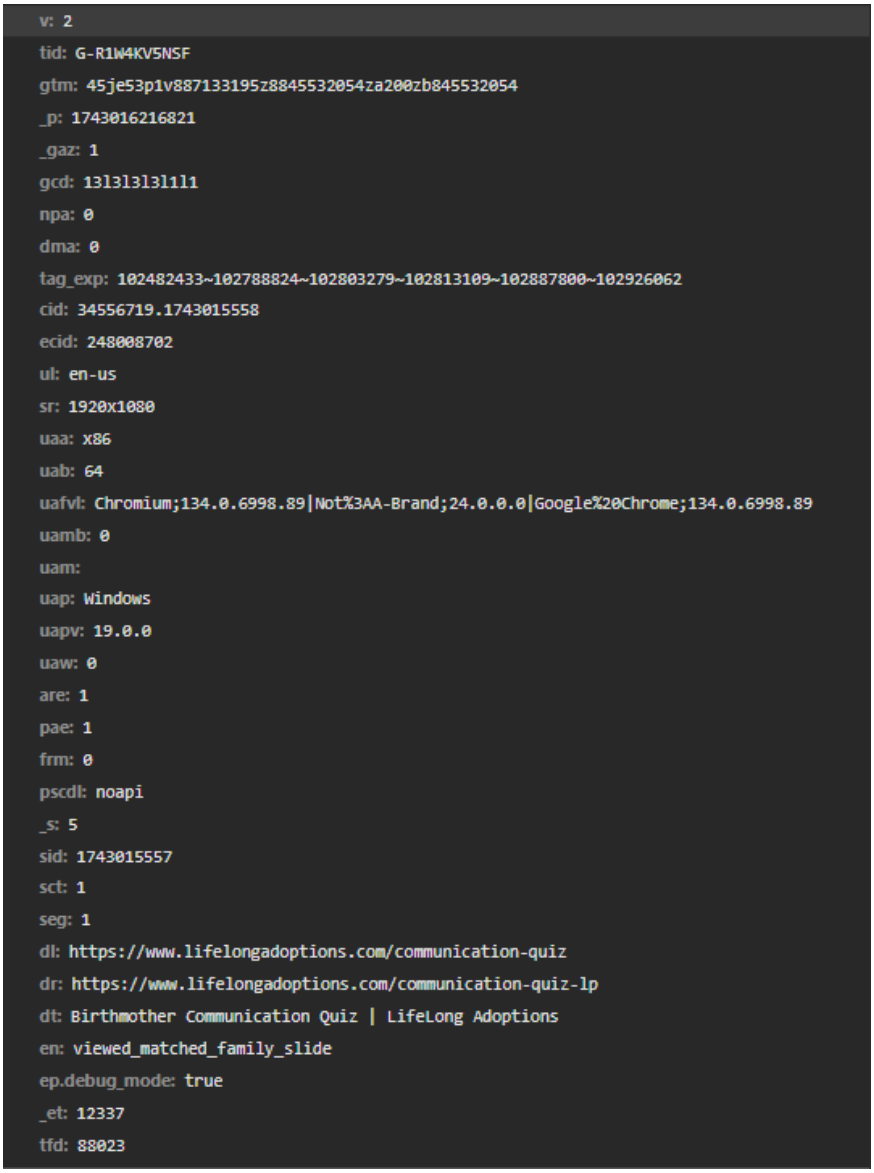

v: 1
_v: j101
a: 469079578
t: event
ni: 0
_s: 1
dl: https://www.lifelongadoptions.com/communication-quiz
ul: en-us
de: UTF-8
dt: Birthmother Communication Quiz | LifeLong Adoptions
sd: 24-bit
sr: 1920x1080
vp: 1021x911
je: 0
ec: Family Finder
ea: Viewed Intro Slide
_u: QACAAEABAAAAACAAI~
jid:
gjid:
cid: 34556719.1743015558
tid: UA-24259407-1
_gid: 745835914.1743015558
gtm: 45He53p1n81N7ZCZ2Lv845532054za200
gcd: 13l3l3l3l1l1
dma: 0
tag_exp: 102482433~102788824~102803279~102813109~102887799~102923816~102926062
z: 97078108

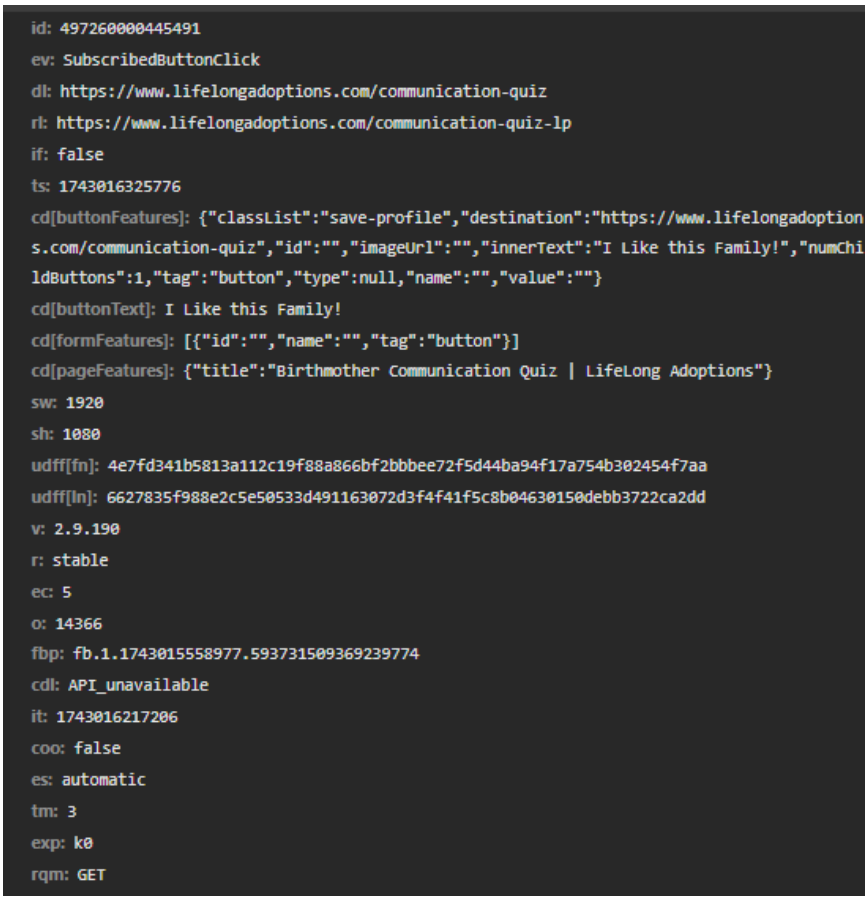

id: 497260000445491
ev: SubscribedButtonClick
dl: https://www.lifelongadoptions.com/communication-quiz-lp
rl: https://www.lifelongadoptions.com/pregnant/why-consider-adoption
if: false
ts: 1743021391078
cd[buttonFeatures]: {"classList":"btn btn-cyan","destination":"https://www.lifelongadoptions.com/communication-quiz","id":"","imageUrl":"","innerText":"Get Started","numChildButtons":0,"tag":"a","type":null,"name":""}
cd[buttonText]: Get Started
cd[formFeatures]: []
cd[pageFeatures]: {"title":"Birthmother Communication | LifeLong Adoptions"}
sw: 1920
sh: 1080
v: 2.9.190
r: stable
ec: 1
o: 12318
fbp: fb.1.1743015558977.593731509369239774
ler: empty
cdl: API_unavailable
it: 1743021390234
coo: false
es: automatic
tm: 3
exp: k0
rqm: GET

Figures 7 & 8. Screenshots depicting back-end network traffic from Defendant's Website which shows information transmitted to Google and Facebook when Website users take Defendant's "Birthmother Communication Quiz."

71. The Tracking Technologies even transmit a Website user's activities while viewing potential families that may want to adopt their child. Defendant's Website includes the "Family Finder" application, which lets mothers who are considering placing their child up for adoption review pictures and self-written bios of families seeking to adopt a child. The Website user then either indicates interest, or lack of interest, in the adoptive family by selecting either "I Like this Family!" or "See My Next Family" in the application. The screenshots below (Figures 9 & 10) show that when a Website user selects the "I Like this Family!" option in Defendant's "Family Finder" application, the Tracking Technologies notify Google and Facebook, either by transmitting that the Website user "matched" with a family or by transmitting that the user clicked the "I Like this Family!" button. A similar transmission is made every time that the Website user clicks the "I Like this Family!" or "See My Next Family" buttons in the Defendant's "Family Finder"

application. And, that choice is transmitted to Google and Facebook, alongside the identifier number attached to Google's "_cid" and "_sid" cookies and Facebook's "fbp" cookie, which identify, and link the user's Website behavior to the user's Google and Facebook accounts, as well as other information that is commonly used to create a browser fingerprint, such as the user's language selection, screen resolution, operating system software and version number, and internet browser software and version number.





Figures 9 & 10. Screenshots depicting back-end network traffic from Defendant's Website which shows information transmitted to Google and Facebook when Website users select between potential adoptive families in Defendant's "Family Finder" application.

72. In their default state, Google and Facebook's Pixels record and transmit only "automatic events," consisting largely of routine user behavior, such as clicking a link, clicking on an advertisement, or viewing a webpage.[47] However, the Google and Facebook's Pixels used on Defendant's Website are not in their default state. Instead, Defendant intentionally configured the Google and Facebook Pixels on its Website to collect and transmit additional user data, including

[47] *Automatically Collected Events*, GOOGLE ANALYTICS HELP, https://support.google.com/analytics/answer/9234069, (last visited on Mar. 26, 2025); *About automatic events*, META BUSINESS HELP CENTER, https://www.facebook.com/business/help/1292598407460746?id=1205376682832142 (last visited on Mar. 26, 2025).

transmitting when Website users' initiate a call from the Website, or their specific selections in the "Family Finder" application.

73. By installing third-party Tracking Tools, including tracking Pixels, on its Website, and by further configuring those Pixels to collect its Website user's Sensitive Information, Defendant knowingly and intentionally caused Plaintiffs' and Class Members' Sensitive Information to be transmitted to third parties, including Google and Facebook.

B. DEFENDANT DISCLOSED PLAINTIFFS' AND CLASS MEMBERS' SENSITIVE INFORMATION TO THIRD PARTIES WITHOUT THEIR KNOWLEDGE OR CONSENT

a. Defendant failed to inform Plaintiffs and Class Members of its disclosure of their Sensitive Information.

74. In its Privacy Policy, LifeLong claims that:

> We will use your information to respond to you regarding the reason you contacted us. We will not share your information with any third party outside of our organization, other than as necessary to fulfill your request.[48]

75. This statement is a lie. In reality, essentially every action taken by a Website user is recorded and transmitted to third party advertisers, including Google and Facebook.

76. Defendant breached Plaintiffs' and Class Members' right to privacy by unlawfully disclosing their Sensitive Information to third parties, including Google and Facebook. Specifically, Plaintiffs and Class Members had a reasonable expectation of privacy, based in-part on Defendant's own representations to Plaintiffs and the Class. Defendant did not inform Plaintiffs and Class Members that it was sharing their Sensitive Information with third parties, including Google and Facebook.

[48] *Privacy Policy*, LIFELONG ADOPTIONS, https://www.lifelongadoptions.com/privacy (last visited on Mar. 26, 2025).

77. By engaging in this improper sharing of information without Plaintiffs' and Class Members' consent, Defendant breached Plaintiffs' and Class Members' right to privacy and unlawfully disclosed their Sensitive Information.

78. Knowing just how invasive it can be when a user's Sensitive Information is disclosed without consent, Facebook explicitly stated, in an action pending against Facebook related to use of its Meta Pixel on a healthcare provider's Website, that it requires Facebook Pixel users to "post a prominent notice on every page where the pixel is embedded and to link from that notice to information about exactly how the pixel works and what is being collected through it, so it is not invisible."[49] Defendant did not abide by this policy.

79. Despite never telling users like Plaintiffs and Class Members, Defendant allowed third parties such as Google and Facebook to intercept Plaintiffs' and Class Members' Sensitive Information and use it for advertising purposes.

b. The Tracking Tools Used by Defendant Were Imperceptible to Plaintiffs and Class Members

80. The Tracking Tools installed on Defendant's Website were invisible to Plaintiffs and Class Members. Without analyzing the network information transmitted by Defendant's Website through examination of its source code or the use of sophisticated web developer tools, there was no way for a Website user to discover the presence of the Tracking Tools. As a result, typical internet users, such as Plaintiffs and Class Members, were unable to detect the Tracking Tools on Defendant's Website.

[49] *See* Transcript of the argument on Plaintiff's Motion for Preliminary Injunction in *In re Meta Pixel Healthcare Litigation*, Case No. CV-22-03580-WHO (N.D. Cal. Nov. 9, 2022) (Hon. J. Orrick), at 19:12-18; *see also In re Meta Pixel Healthcare Litig.*, 2022 WL 17869218 (N.D. Cal. Dec 22, 2022).

81. Plaintiffs and Class Members were shown no disclaimer or warning that their Sensitive Information would be disclosed to any unauthorized third party without their express consent.

82. Plaintiffs and Class Members did not know that their Sensitive Information was being collected and transmitted to an unauthorized third party.

83. Because Plaintiffs and Class Members were not aware of the Google and Facebook Pixels on Defendant's website, or that their Sensitive Information would be collected and transmitted to Google and Facebook, they could not and did not consent to Defendant's conduct.

C. DEFENDANT WAS ENRICHED BY ITS DISCLOSURE OF PLAINTIFFS' AND CLASS MEMBERS' SENSITIVE INFORMATION TO THIRD PARTIES

a. Defendant Received Material Benefits in Exchange for Plaintiffs' Sensitive Information

84. As explained, *supra*, users of Google and Facebook's Business Tools, like Defendant, receive access to advertising and marketing analytics services in exchange for installing Google and Facebook's Tracking Tools on their website.

85. Upon information and belief, Defendant, as a user of Google and Facebook's Business Tools, received compensation in the form of advanced advertising services and cost-effective marketing on third-party platforms in exchange for allowing Google and Facebook to collect Plaintiffs' and Class Members' Sensitive Information.

b. Plaintiffs' and Class Members' Data Had Financial Value

86. Moreover, Plaintiffs' and Class Members' Sensitive Information had value, and Defendant's disclosure and interception of that Sensitive Information harmed Plaintiffs and the Class.

87. According to Facebook's annual reports, the value it derives from user data has continuously risen. "In 2013, the average American's data was worth about $19 per year in

advertising sales to Facebook, according to its financial statements. In 2020, [it] was worth $164 per year."[50]

88. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

89. Several companies have products through which they pay consumers for a license to track certain information. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing history information.

90. Facebook itself has paid users for their digital information, including browsing history. Until 2019, Facebook ran a "Facebook Research" app through which it paid $20 a month for a license to collect browsing history information and other communications from consumers between ages 13 and 35.[51]

91. The unauthorized disclosure of Plaintiffs' and Class Members' private and Sensitive Information has diminished the value of that information, resulting in harm to Plaintiffs and Class Members.

D. PLAINTIFFS' AND CLASS MEMBERS' REASONABLE EXPECTATION OF PRIVACY

92. At all times when Plaintiffs and Class Members provided their Sensitive Information to Defendant, they each had a reasonable expectation that the information would

[50] Geoffrey A. Fowler, *There's no escape from Facebook, even if you don't use it*, THE WASHINGTON POST (Aug. 29, 2021), https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/ (last visited Mar. 26, 2025).

[51] Louis Matsakis, WIRED (Jan. 30, 2019), https://www.wired.com/story/facebook-research-app-root-certificate/ (last visited Feb. 2, 2025).

remain confidential and that Defendant would not share the Sensitive Information with third parties for a commercial purpose, unrelated to providing them with access to adoption services.

93. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative informed consent before a company collects and shares that individual's data to be one of the most important privacy rights.

94. For example, a recent Consumer Reports study shows that 92-percent of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[52]

95. Americans are particularly sensitive about disclosing information related to unintended pregnancy. Indeed, numerous studies have noted that feelings of intense shame are often experienced by mothers experiencing unintended pregnancy, particularly due to the intense social stigma attached in many communities.[53]

96. Personal data privacy and obtaining consent to share Sensitive Information are material to Plaintiffs and Class Members.

V. TOLLING AND ESTOPPEL

97. Any applicable statutes of limitation have been tolled by Defendant's knowing and active concealment of its incorporation of Google and Facebook's Tracking Tools into its Website.

---

[52] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907 (last visited Mar. 26, 2025).

[53] *See, e.g.,* Whitney Smith, Janet M Turan, Kari White, Kristi L Stringer, Anna Helova, Tina Simpson, & Kate Cockrill, *Social Norms and Stigma Regarding Unintended Pregnancy and Pregnancy Decisions: A Qualitative Study of Young Women in Alabama*, PERSP. SEX REPROD. HEALTH. (2018), *available online at*: https://pmc.ncbi.nlm.nih.gov/articles/PMC5022769/.

98. The Pixels and other tracking tools on Defendant's Website were and are invisible to the average website visitor.

99. Through no fault or lack of diligence, Plaintiffs and Class Members were deceived and could not reasonably discover Defendant's deception and unlawful conduct.

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

101. Defendant had exclusive knowledge that its Website incorporated the Pixels and other Tracking Tools and yet failed to disclose to customers, including Plaintiffs and Class Members, that by requesting a consultation via the Website, Plaintiffs' and Class Members' Sensitive Information would be disclosed or released to unauthorized third parties, including Google and Facebook.

102. Under the circumstances, Defendant was under a duty to disclose the nature, significance, and consequences of its collection and treatment of its customers' Sensitive Information. In fact, to the present, Defendant has not conceded, acknowledged, or otherwise indicated to its customers that it has disclosed or released their Sensitive Information to unauthorized third parties. Accordingly, Defendant is estopped from relying on any statute of limitations.

103. Moreover, all applicable statutes of limitation have also been tolled pursuant to the discovery rule.

104. The earliest that Plaintiffs or Class Members, acting with due diligence, could have reasonably discovered Defendant's conduct would have been shortly before the filing of this Complaint.

VI. CLASS ALLEGATIONS

105. This action is brought by the named Plaintiffs on their own behalf, and on behalf of a proposed Class of all other persons similarly situated under Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

106. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

The Nationwide Class

All natural persons who used Defendant's Website to research their options in connection with a pregnancy, request information, request a consultation, use the "Family Finder" application, or take the "Birthmother Communication Quiz," and whose Sensitive Information was disclosed or transmitted to Facebook, Google, or any other unauthorized third party.

107. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of separate California and Pennsylvania Subclasses, which are defined as follows:

California Subclass

All natural persons residing in the State of California who used Defendant's Website to research their options in connection with a pregnancy, request information, request a consultation, use the "Family Finder" application, or take the "Birthmother Communication Quiz," and whose Sensitive Information was disclosed or transmitted to Facebook, Google, or any other unauthorized third party.

Pennsylvania Subclass

All natural persons residing in the State of Pennsylvania who used Defendant's Website to research their options in connection with a pregnancy, request information, request a consultation, use the "Family Finder" application, or take the "Birthmother Communication Quiz," and whose Sensitive Information was disclosed or transmitted to Facebook, Google, or any other unauthorized third party.

108. Excluded from the proposed Classes are any claims for personal injury, wrongful death, or other property damage sustained by the Classes; and any Judge conducting any proceeding in this action and members of their immediate families.

109. Plaintiffs reserve the right to amend the definitions of the Classes or add subclasses if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

110. **Numerosity.** The Class is so numerous that the individual joinder of all members is impracticable. There are at least 1,000 individuals that have been impacted by Defendant's actions. Moreover, the exact number of those impacted is generally ascertainable by appropriate discovery and is in the exclusive control of Defendant.

111. **Commonality.** Common questions of law or fact arising from Defendant's conduct exist as to all members of the Class, which predominate over any questions affecting only individual Class Members. These common questions include, but are not limited to, the following:

a) Whether and to what extent Defendant had a duty to protect the Sensitive Information of Plaintiffs and Class Members;

b) Whether Defendant had duties not to disclose the Sensitive Information of Plaintiffs and Class Members to unauthorized third parties;

c) Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Sensitive Information would be disclosed to third parties;

d) Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Sensitive Information was being disclosed without their consent;

e) Whether Defendant adequately addressed and fixed the practices which permitted the unauthorized disclosure of Website users' Sensitive Information;

f) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to keep the Sensitive Information belonging to Plaintiffs and Class Members free from unauthorized disclosure;

g) Whether Defendant violated the statutes asserted as claims in this Complaint;

h) Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

i) Whether Defendant knowingly made false representations as to its data security and/or privacy practices;

j) Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy practices; and

k) Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendant's disclosure of their Sensitive Information.

112. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Sensitive Information, like that of every other Class Member, was compromised as a result of Defendant's incorporation and use of the Tracking Tools.

113. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

114. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members in that all the Plaintiffs' and Class Members' data was unlawfully stored and disclosed to unauthorized third parties, including third parties like Google and Facebook, in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

115. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

116. Defendant acted on grounds that apply generally to the Class as a whole so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

117. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a) Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Sensitive Information and not disclosing it to unauthorized third parties;

b) Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Sensitive Information;

c) Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d) Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Sensitive Information would be disclosed to third parties;

e) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

f) Whether Class Members are entitled to actual, consequential, and/or nominal damages and/or injunctive relief as a result of Defendant's wrongful conduct.

118. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the unauthorized disclosures that have taken place.

COUNT I
COMMON LAW INVASION OF PRIVACY - INTRUSION UPON SECLUSION
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California and/or Pennsylvania Subclasses)

119. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 118 as if fully set forth herein.

120. Plaintiffs and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their confidential and/or highly personal Sensitive Information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to the exfiltration of their communications without Plaintiffs' and Class Members' knowledge or consent.

121. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website and the communications platforms and services therein.

122. Plaintiffs and Class Members communicated Sensitive Information that they

intended for only Defendant to receive and that they understood Defendant would keep private and secure.

123. Defendant's disclosure of the substance and nature of those communications to third parties, including Google and Facebook, without the knowledge and informed consent of Plaintiffs and Class Members is an intentional intrusion on Plaintiffs' and Class Members' solitude or seclusion.

124. Plaintiffs and Class Members had a reasonable expectation of privacy, which included that their communications regarding sensitive, highly personal information would be protected from surreptitious disclosure to third parties.

125. Defendant's disclosure of Plaintiffs' and Class Members' Sensitive Information coupled with individually identifying information is highly offensive to the reasonable person.

126. As a result of Defendant's actions, Plaintiffs and Class Members have suffered harm and injury including, but not limited to, an invasion of their privacy rights.

127. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to compensatory and/or nominal damages.

128. Plaintiffs and Class Members seek appropriate relief for that injury including, but not limited to, damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as a result of the intrusions upon their privacy.

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

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

COUNT II
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California and/or Pennsylvania Subclasses)

131. Plaintiffs repeat and reallege the allegations contained in paragraphs 119 through 130 as if fully set forth herein.

132. Plaintiffs and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

133. Plaintiffs' and Class Members' reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises of confidentiality on its Website.

134. Contrary to its duties and its express promises of confidentiality, Defendant deployed the Tracking Technologies to disclose and transmit Plaintiffs' and Class Members' Sensitive Information and the contents of their communications exchanged with Defendant to third parties.

135. The third-party recipients included, but were not limited to, Google, Facebook,and other online marketers.

136. Defendant's disclosures of Plaintiffs' and Class Members' Sensitive Information were made without their knowledge, consent or authorization, and were unprivileged.

137. The harm arising from a breach of confidentiality includes erosion of the essential confidential relationship between the provider and client.

138. As a direct and proximate cause of Defendant's unauthorized disclosures of personally identifiable, non-public information, and communications, Plaintiffs and Class Members were damaged by Defendant's breach in that:

a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of the provider-provider-client relationship;

c. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensating Plaintiffs and Class Members for the data;

d. Defendant's actions diminished the value of Plaintiffs' and Class Members' Sensitive Information, and

e. Defendant's actions violated the property rights Plaintiffs and Class Members have in their Sensitive Information.

139. Plaintiffs and Class Members are therefore entitled to general damages for invasion of their rights in an amount to be determined by a jury and nominal damages for each independent violation. Plaintiffs are also entitled to punitive damages.

COUNT II
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California and/or Pennsylvania Subclasses)

140. Plaintiffs repeat and reallege the allegations contained in paragraphs 131 through 139 as if fully set forth herein.

141. In light of the special relationship between Defendant on the one hand and Plaintiffs and Class Members on the other hand, whereby Defendant became guardian of Plaintiffs' and Class Members' Sensitive Information, Defendant became a fiduciary by its undertaking and guardianship of the Sensitive Information, to act primarily for Plaintiffs and Class Members: (1) for the safeguarding of Plaintiffs' and Class Members' Sensitive Information; (2) to timely notify Plaintiffs and Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

142. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with its clients and potential clients, and in particular, to keep their Sensitive Information secure.

143. Defendant breached its fiduciary duties to Plaintiffs and Class Members by disclosing their Sensitive Information to unauthorized third parties, including Google and Facebook, and separately, by failing to notify Plaintiffs and Class Members of this fact.

144. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer injury and are entitled to compensatory, nominal, and/or punitive damages, and disgorgement of profits, in an amount to be proven at trial.

COUNT IV
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California and/or Pennsylvania Subclasses)

145. Plaintiffs repeat and reallege the allegations contained in paragraphs 140 through 144 as if fully set forth herein.

146. Through using Defendant's Website, Plaintiffs and Class Members provided it with their Sensitive Information.

147. By collecting and storing this data, Defendant had a duty of care to use reasonable means to secure and safeguard it from unauthorized disclosure to third parties, including Google and Facebook.

148. Defendant negligently failed to take reasonable steps to protect Plaintiffs' and Class Members' Sensitive Information from being disclosed to third parties, without their consent, including to Google and Facebook.

149. Defendant further negligently omitted to inform Plaintiffs and the Class that it

would use their Sensitive Information for marketing purposes, or that their Sensitive Information would be transmitted to third parties, including Google and Facebook.

150. Defendant knew, or reasonably should have known, that Plaintiffs and the Class would not have provided their Sensitive Information to Defendant, had Plaintiffs and the Class known that Defendant intended to use that information for unlawful purposes.

151. Defendant's conduct has caused Plaintiffs and the Class to suffer damages by having their highly personal, personally identifiable Sensitive Information accessed, stored, and disseminated without their knowledge or consent.

152. Plaintiffs and Class Members are entitled to compensatory, nominal, and/or punitive damages.

153. Defendant's negligent conduct is ongoing, in that it still holds the Sensitive Information of Plaintiffs and Class Members in an unsafe and unsecure manner. Therefore, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; and (ii) submit to future annual audits of those systems and monitoring procedures.

COUNT V
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California and/or Pennsylvania Subclasses)

154. Plaintiffs repeat and reallege the allegations contained in paragraphs 145 through 153 as if fully set forth herein.

155. When Plaintiffs and Class Members provided their Sensitive Information to Defendant in exchange for services, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Sensitive Information without consent.

156. Plaintiffs and Class Members accepted Defendant's offers and provided their

Sensitive Information to Defendant.

157. Plaintiffs and Class Members would not have entrusted Defendant with their Sensitive Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Sensitive Information without consent.

158. Defendant breached these implied contracts by disclosing Plaintiffs' and Class Members' Sensitive Information to third parties like Google and Facebook.

159. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein.

160. Plaintiffs and Class Members are entitled to compensatory, consequential, and/or nominal damages as a result of Defendant's breaches of implied contract.

COUNT VI
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California and/or Pennsylvania Subclasses)

161. Plaintiffs repeat and reallege the allegations contained in paragraphs 154 through 160 as if fully set forth herein.

162. Plaintiffs plead this claim in the alternative to their breach of implied contract claim.

163. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided their Sensitive Information to Defendant, which it exchanged for marketing and advertising services, including to Google and Facebook, as described, *supra*.

164. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from the Sensitive Information of Plaintiffs and Class Members by exchanging it for marketing and advertising services.

165. In particular, Defendant enriched itself by obtaining the inherent value of Plaintiffs'

and Class Members' Sensitive Information, and by saving the costs it reasonably should have expended on marketing and/or data security measures to secure Plaintiffs' and Class Members' Sensitive Information.

166. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the privacy of their Sensitive Information.

167. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, obtained by its surreptitious collection and transmission of their Sensitive Information.

168. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Sensitive Information, they would not have agreed to provide their Sensitive Information to Defendant.

169. Plaintiffs and Class Members have no adequate remedy at law for this count. An unjust enrichment theory provides the equitable disgorgement of profits even where an individual has not suffered a corresponding loss in the form of money damages.

170. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer injury.

171. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them, or to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

COUNT VII
VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. § 2511(1), *et seq*.

(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California and/or Pennsylvania Subclasses)

172. Plaintiffs repeat and reallege the allegations contained in paragraphs 161 through 171 as if fully set forth herein.

173. The ECPA protects both sending and receipt of communications.

174. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

175. The transmissions of Plaintiff's Sensitive Information to Defendant's Website qualify as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

176. Electronic Communications. The transmission of Sensitive Information between Plaintiffs and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

177. Content. The ECPA defines content, when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

178. Interception. The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

179. Electronic, Mechanical or Other Device. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices;

c. Defendant's web-servers; and

d. The Pixel code deployed by Defendant to effectuate the sending and acquisition of sensitive communications.

180. By utilizing and embedding the Pixels on its Website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

181. Specifically, Defendant intercepted Plaintiffs' and Class Members' electronic communications via the Pixels, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' Private Information to third parties such as Google and Facebook.

182. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs and Class Members regarding their Sensitive Information, including the fact that Plaintiffs and Class Members sought assistance with a consultation from Defendant regarding placing their child up for adoption.

183. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

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

185. Unauthorized Purpose. Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, invasion of privacy, among others.

186. The ECPA provides that a "party to the communication" may be liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

187. Defendant is not a party to the communication, for purposes of the ECPA, based on its unauthorized duplication and transmission of communications with Plaintiffs and the Class. However, even assuming Defendant is a party, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiffs' and Class Members' Sensitive Information does not qualify for the party exemption.

188. Defendant's acquisition of sensitive communications that were used and disclosed to Google was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and individual States nationwide as set forth herein, including:

a. Invasion of privacy;

b. Breach of confidence;

c. Breach of fiduciary duty;

d. The California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.:*

e. The Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. § 5702; 5703, *et seq*.; and

f. The Pennsylvania Unfair Trade Practice and Consumer Protection Law, 73 Pa. Stat. Ann. § 201-1, *et seq*.

189. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it: Used and caused to be used cookie identifiers associated with specific users, including Plaintiffs and Class Members, without user authorization; and disclosed individually identifiable Sensitive Information to Google and Facebook without user authorization.

190. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiffs' and Class Members' communications about their Sensitive Information on its Website, because it used its participation in these communications to improperly share Plaintiffs' and Class Members' Private Information with Google, Facebook, and third-parties that did not participate in these communications, that Plaintiffs and Class Members did not know were receiving their Sensitive Information, and that Plaintiffs and Class Members did not consent to receive their Sensitive Information.

191. As such, Defendant cannot viably claim any exception to ECPA liability.

192. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their Sensitive Information for commercial purposes has caused Plaintiffs and Class Members to suffer emotional distress;

b. Defendant received substantial financial benefits from its use of Plaintiffs' and Class Members' Sensitive Information without providing any value or benefit to Plaintiffs or Class Members;

c. Defendant received substantial, quantifiable value from its use of Plaintiffs' and Class Members' Sensitive Information, such as understanding how

people use its Website and determining what ads people see on its Website, without providing any value or benefit to Plaintiffs or Class Members;

d. The diminution in value of Plaintiffs' and Class Members' Sensitive Information and/or the loss of privacy due to Defendant making such Sensitive Information, which Plaintiffs and Class Members intended to remain private, no longer private.

193. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixels to track and utilize Plaintiffs' and Class Members' Sensitive Information for financial gain.

194. Defendant was not acting under color of law to intercept Plaintiff's and the Class Members' wire or electronic communication.

195. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading their privacy via the Tracking Tools.

196. Any purported consent that Defendant may claim it received from Plaintiffs and Class Members was not valid.

197. In sending and acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of Defendant's Website, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions including a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

198. As a result of Defendant's violation of the ECPA, Plaintiffs and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT VIII
INVASION OF PRIVACY UNDER CALIFORNIA'S CONSTITUTION

Cal. Const. Art. 1, § 1
(On Behalf of Plaintiff E.H. and the California Subclass)

199. Plaintiffs repeat and reallege the allegations contained in paragraphs 172 through 198 as if fully set forth herein.

200. Article I, section 1 of the California Constitution provides that "[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

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

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

203. Defendant violated Plaintiff E.H.'s and California Subclass Members' constitutional right to privacy by collecting, storing and disclosing their personal information in which they had a legally protected privacy interest and for which they had a reasonable expectation of privacy, in a manner that was highly offensive to Plaintiff E.H. and California Subclass Members and was an egregious violation of social norms.

204. Defendant has intruded upon Plaintiff's and Subclass Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential Personal Information.

205. Plaintiff E.H. and California Subclass Members had a reasonable expectation of privacy in that: (i) Defendant's invasion of privacy occurred as a result of Defendant's security

practices, including the collecting, storage, and unauthorized disclosure of consumers' Sensitive Information; (ii) Plaintiff E.H. and California Subclass Members did not consent to or otherwise authorize Defendant to disclose their Sensitive Information; and (iii) Plaintiff E.H. and California Subclass Members could not reasonably expect Defendant would commit acts in violation of privacy protection laws.

206. As a direct and proximate result of Defendant's invasion of their privacy, Plaintiff E.H. and California Subclass Members have been damaged and have suffered actual and concrete injuries.

207. Plaintiff E.H. and California Subclass Members are entitled to appropriate relief, including damages to compensate them for the harm to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, risk of future invasions of privacy and the mental and emotional distress and harm to human dignity interests caused by Defendant's invasions.

208. Plaintiff E.H. and California Subclass Members seek appropriate relief for that injury including, but not limited to, damages that will reasonably compensate Plaintiff E.H. and California Subclass Members for the harm to their privacy interests, nominal damages, and/or disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiff's and Class Members' privacy.

COUNT IX
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq*. - Unfair Business Practices
(*On behalf of Plaintiff E.H. and the California Subclass*)

209. Plaintiffs repeat and reallege the allegations contained in paragraphs 199 through 208 as if fully set forth herein.

210. Defendant's business acts and practices meet the unfairness prong of the UCL according to all three theories of unfairness.

211. First, Defendant's business acts and practices are "unfair" under the UCL pursuant to the three-part test articulated in *Camacho v. Automobile Club of Southern California* (2006) 142 Cal. App. 4th 1394, 1403: (a) Plaintiff E.H. and California Subclass Members suffered substantial injury due to Defendant's disclosure of their Sensitive Information; (b) Defendant's disclosure of Plaintiff E.H's and California Subclass Members' Sensitive Information provides no benefit to consumers, let alone any countervailing benefit that could justify Defendant's disclosure of Sensitive Information without consent for marketing purposes or other pecuniary gain; and (c) Plaintiff E.H. and California Subclass Members could not have readily avoided this injury because they had no way of knowing that Defendant was implementing the Pixels. Thus, Plaintiff E.H. and California Subclass Members did not know to ask Defendant to stop the practice of disclosing their Sensitive Information and did not know that they should stop using Defendant's services to avoid disclosing their Sensitive Information

212. Second, Defendant's business acts and practices are "unfair" under the UCL because they are "immoral, unethical, oppressive, unscrupulous, or substantially injurious" to Plaintiff E.H. and California Subclass Members, and "the utility of [Defendant's] conduct," if any, does not "outweigh the gravity of the harm" to Plaintiff E.H.'s and California Subclass Members' *Drum v. San Fernando Valley Bar Ass'n*, 182 Cal. App. 4th 247, 257 (2010). Defendant engaged in unfair business practices by disclosing Plaintiffs' and Subclass Members' Sensitive Information to unrelated third parties, including Google and Facebook, without prior consent despite its promises to keep such information confidential. This surreptitious and undisclosed conduct is immoral, unethical, oppressive, unscrupulous, and substantially injurious. No benefit inheres in this conduct, the gravity of which is significant.

213. Third, Defendant's business acts and practices are "unfair" under the UCL because they run afoul of "specific constitutional, statutory, or regulatory provisions." *Drum*, 182 Cal. App. 4th at 256 (internal quotation marks and citations omitted). California has a strong public policy of protecting consumers' privacy interests, including consumers' personal data. This public policy is codified in California's Constitution in Article I, section 1; CIPA, Cal. Penal Code §§ 630, *et seq*.; the CMIA, Cal. Civil Code §§ 56.06, 56.10, 56.101; and the California Consumer Privacy Act, Cal. Civil Code §§ 1798, *et seq*., among other statutes.

214. This public policy is further codified on a nationwide basis in federal statutes, including the FTC Act and the ECPA. Defendant violated this public policy by, among other things, surreptitiously collecting, disclosing, and otherwise exploiting Plaintiffs' and Subclass Members' Sensitive Information by sharing it with Facebook and other third parties via the Pixels without Plaintiffs' and/or Class Members' consent.

215. Plaintiff E.H. and California Subclass Members understood that Defendant, as a provider aiding vulnerable persons, would take appropriate measures to keep their Sensitive Information private and confidential.

216. In its privacy policies, Defendant promised that it would not share Plaintiff E.H.'s and California Subclass Members' private information with any third party without consent or for marketing purposes. Contrary to its own policies, Defendant did disclose Plaintiff's and Subclass Members' Sensitive Information to third parties without consent and for marketing purposes. Defendant was in sole possession of and had a duty to disclose the material information that Plaintiff E.H.'s and California Subclass Members' Sensitive Information was being shared with a third party.

217. Had Defendant disclosed that it shared Sensitive Information with third parties, Plaintiff E.H. would not have used Defendant's services.

218. The harm caused by the Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests other than Defendant's conduct described herein.

219. Plaintiff E.H. and California Subclass Members trusted Defendant to keep their Sensitive Information confidential, and as a result, shared highly sensitive information through their use of the Website, causing them to suffer damages when Defendant disclosed that information to third parties.

220. As a direct and proximate result of Defendant's violations of the UCL, Plaintiff E.H. and California Subclass Members have suffered injury in fact and lost money or property, including, but not limited to, payments Plaintiff E.H. and California Subclass Members made to Defendant and/or other valuable consideration, such as access to their private and personal data. Plaintiff E.H. and California Subclass Members also lost the value of their Sensitive Information as a result of Defendant's unfair business practices.

221. As a direct result of its unfair practices, Defendant has been unjustly enriched and should be required to make restitution to Plaintiff E.H. and California Subclass Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code, restitutionary disgorgement of all profits accruing to Defendant because of its unlawful business practices, declaratory relief, attorney fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

222. In the alternative to those claims seeking remedies at law, Plaintiff E.H. alleges that there is no plain, adequate, and complete remedy that exists at law to address Defendant's unlawful

and unfair business practices. The legal remedies available to Plaintiff E.H. are inadequate because they are not "equally prompt and certain and in other ways efficient" as equitable relief. *American Life Ins. Co. v. Stewart*, 300 U.S. 203, 214 (1937); *see also United States v. Bluitt*, 815 F. Supp. 1314, 1317 (N.D. Cal. Oct. 6, 1992) ("The mere existence' of a possible legal remedy is not sufficient to warrant denial of equitable relief.").

223. Additionally, unlike damages, the Court's discretion in fashioning equitable relief is very broad and can be awarded in situations where the entitlement to damages may prove difficult. *Cortez v. Purolator Air Filtration Products Co.*, 23 Cal.4th 163, 177-180 (2000) (Restitution under the UCL can be awarded "even absent individualized proof that the claimant lacked knowledge of the overcharge when the transaction occurred.").

224. Thus, restitution would allow recovery even when normal consideration associated with damages would not. *See, e.g., Fladeboe v. Am. Isuzu Motors Inc.*, 150 Cal. App. 4th 42, 68 (2007) (noting that restitution is available even in situations where damages may not be available). Furthermore, the standard for a violation of the UCL "unfair" prong is different from the standard that governs legal claims.

COUNT X
VIOLATIONS OF THE PENNSYLVANIA WIRETAPPING AND ELECTRONIC SURVEILLANCE CONTROL ACT ("WESCA")
18 Pa. Cons. Stat. § 5702; 5703, *et seq*.
(On Behalf of Plaintiff V.P. and the Pennsylvania Subclass)

225. Plaintiffs repeat and reallege the allegations contained in paragraphs 209 through 224 as if fully set forth herein.

226. The WESCA prohibits any person from "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[.]" 18 Pa. Cons. Stat. Ann. § 5703(1).

227. Defendant, Google, and Facebook are "persons" under 18 Pa. Cons. Stat. § 5702.

228. The Private Information communicated to Defendant by Plaintiff V.P. and Pennsylvania Subclass Members through their use of the Website are "electronic communications" under 18 Pa. Cons. Stat. § 5702.

229. Defendant violated the WESCA by knowingly enabling Google and Facebook's interception of Plaintiff V.P.'s and Pennsylvania Subclass Members' electronic communications by installing the Tracking Tools on its Website.

230. As a result of Defendant's violation of the WESCA, Plaintiff V.P. and Pennsylvania Subclass Members are entitled to all damages available under 18 Pa. Cons. Stat. § 5725, including actual damages, statutory damages of up to $1,000 per violation, punitive damages, and attorney's fees and costs.

COUNT XI
VIOLATIONS OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW ("UTPCPL")
73 Pa. Stat. Ann. § 201-1, *et seq*.
(On Behalf of Plaintiff V.P. and the Pennsylvania Subclass)

231. Plaintiffs repeat and reallege the allegations contained in paragraphs 225 through 230 as if fully set forth herein.

232. The UTPCPL prohibits anyone from "[e]ngaging in any[]fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding." 73 Pa. Stat. Ann. § 201-2.

233. Defendant's knowing, intentional violations of the UTPCPL include:

i. Falsely promising that it would keep confidential and not disclose Plaintiff V.P.'s and Pennsylvania Subclass Members' Sensitive Information;

ii. Failing to inform Plaintiff V.P. and Pennsylvania Subclass Members that it would provide their Sensitive Information to third parties in exchange for advertising and marketing services; and

iii. Surreptitiously collecting and sharing Plaintiff V.P.'s and Pennsylvania Subclass Members' with third parties.

234. As a result of Defendant's violation of the UTPCPL, Plaintiff V.P. and Pennsylvania Subclass Members are entitled to all damages available under 73 Pa. Stat. Ann. § 201-9.2, including statutory damages of up to $100 per violation, equitable or declaratory relief, compensatory and treble damages, and attorney's fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, pray for judgment against Defendant as follows:

A. an Order certifying the Nationwide Class, and California and Pennsylvania Subclasses, and appointing the Plaintiffs and their Counsel to represent the Classes;
B. equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Sensitive Information of Plaintiffs and Class Members;
C. injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;
D. an award of all damages available at equity or law, including, but not limited to, actual, consequential, punitive, statutory and nominal damages, as allowed by law in an amount to be determined;
E. an award of attorney fees, costs, and litigation expenses, as allowed by law;
F. prejudgment interest on all amounts awarded; and
G. all such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and other members of the proposed Classes, hereby demand a jury trial on all issues so triable.

Dated: April 16, 2025

Respectfully submitted,

/s/ Catherine E. Ybarra
Catherine E. Ybarra (SBN # 283360)
cybarra@sirillp.com
SIRI & GLIMSTAD LLP
700 S. Flower Street, Ste. 1000
Los Angeles, CA 90017
Telephone: (213) 376-3739

Tyler J. Bean*
Sonjay C. Singh*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: tbean@sirillp.com
E: ssingh@sirillp.com

**pro hac vice admission anticipated*

Attorneys for Plaintiffs and the Class

ClassAction.org