BURSOR & FISHER, P.A.
Philip L. Fraietta (State Bar No. 354768)
50 Main Street, Suite 475
White Plains, NY 10606
Telephone: (914) 874-0708
Facsimile: (914) 206-3656
E-mail: pfraietta@bursor.com

BURSOR & FISHER, P.A.
Max S. Roberts (State Bar No. 363482)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: mroberts@bursor.com

BURSOR & FISHER, P.A.
Joshua R. Wilner (State Bar No. 353949)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: jwilner@bursor.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

AUSTIN SKAGGS, individually and on behalf of all others similarly situated, Plaintiff, v. X.AI, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Austin Skaggs ("Plaintiff") brings this action on behalf of himself and all others similarly situated against X.AI, LLC ("Defendant" or "X"). Plaintiff brings this action based upon personal knowledge of the facts pertaining to himself, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. This is a class action lawsuit brought on behalf of all United States residents who have accessed and entered queries into Grok.com (the "Website"), a website Defendant owns and operates.

2. Defendant owns and operates Grok, an AI chatbot service designed to provide answers to almost any question a user asks, including queries regarding sensitive and personal topics like the user's finances, health, and legal issues.

3. Despite reasonable expectations of privacy, and Defendant's legal duties to prevent the disclosure of such private information, Defendant disclosed nearly every piece of information provided by consumers to Google, LLC ("Google"), Meta Platforms, Inc. ("Meta"), and TikTok, Inc. ("TikTok") (together the "Third Parties") by incorporating technology owned by the Third Parties into the code of its website.

4. Through the acts alleged herein, Defendant violated the Electronic Communications Privacy Act, 18 U.S.C. 2511, *et seq*. ("ECPA"), the California Invasion of Privacy Act ("CIPA") §§ 631 and 632, and the California Constitution and Common Law by disclosing Plaintiff's and Class Members' private and confidential information without consent.

PARTIES

Defendant

5. Defendant X.AI, LLC is a Nevada Limited Liability Corporation with its principal place of business at 1450 Page Mill Road Palo Alto, CA, 94304. Defendant owns and operates the Website.

Plaintiff

6. Plaintiff Austin Skaggs is a natural person and citizen of California, residing in Modesto, California.

7. Throughout 2025 and 2026, including as recently as May 2026, Plaintiff visited the Website and entered queries related to sensitive information about finances, investment strategy, private health conditions, business projects, and other private information.

8. Plaintiff has had an active Facebook account for several years. Plaintiff routinely accesses Facebook on his computer using the same browser he used to access the Website.

9. Plaintiff also has had an active Google account for several years and is routinely logged into that account while using the same browser they used to access the Website.

10. Pursuant to the systematic process described herein, Defendant aided and assisted Google with intercepting Plaintiff's communications, including those that contained personally identifiable information ("PII"), and related confidential information. Defendant aided and assisted these interceptions without Plaintiff's knowledge, consent, or express written authorization.

11. By failing to receive the requisite consent, Defendant breached its duties of confidentiality and unlawfully disclosed Plaintiff's PII and confidential communications.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000, exclusive of interest and costs, and at least one member of the proposed class is a citizen of a state different from at least one Defendant.

13. This Court has personal jurisdiction over Defendant because the Website collected and disseminated the information giving rise to this lawsuit in this District, Defendant conducts substantial business in this District, Defendant's Website allows California residents to use the Website in California, and the conduct giving rise to this action arises out of and relates to that business.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events giving rise to the claim occurred in this District, and Defendant resides in this District.

FACTUAL ALLEGATIONS

A. Background of the California Information Privacy Act ("CIPA")

15. The CIPA, Cal. Penal Code § 630, *et seq.*, prohibits aiding or permitting another person to willfully—and without the consent of all parties to a communication—read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from or received at any place within California.

16. To establish liability under Cal. Penal Code § 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> Or
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,
>
> Or
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

17. The applicability of Cal. Penal Code Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589

(9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' internet browsing history).

18. Under Cal. Penal Code § 637.2, Plaintiff and Class Members may seek injunctive relief and statutory damages of $5,000 per violation.

B. Defendant's Website

19. Defendant's Website hosts Grok, "an AI chatbot and large language model (LLM). Developed by xAI, owned by Elon Musk."[1] "According to xAI's website, 'Grok is your truth-seeking AI companion for unfiltered answers with advanced capabilities in reasoning, coding, and visual processing.'"[2]

20. Users enter queries on virtually any topic into the Website and receive conversational responses in writing with answers to their questions. Millions of people use Grok to get answers in the way people have become accustomed to searching for information on search engines.

21. Unlike other conversational AI services, the Grok website is designed such that each query and resulting conversation, including every question by the user and answer by Grok, is assigned a unique URL. The privacy implication of this is any party that Grok shares the URL with is able to obtain a full transcript of the conversation.

C. Overview of the Wiretaps

1. Google Analytics' Tracking Code

22. "Google Analytics is a platform that collects data from [] websites and apps to create reports that provide insights into [] business[es]."[3]

23. To discern when "two different [users] interact with [a] website[,] … Google Analytics identifies an individual user based on [Google Analytics] reporting identit[ies.]"[4]

---

[1] What is Grok? Is it safe for kids?, gabb.Now, https://gabb.com/blog/grok/.

[2] *Id*.

[3] GOOGLE, HOW GOOGLE ANALYTICS WORKS, https://support.google.com/analytics/answer/12159447.

[4] GOOGLE, TRAFFIC-SOURCE DIMENSIONS, https://support.google.com/analytics/answer/11080067.

Reporting identities are combinations of "identifiers … called *identity spaces*"—namely, "User-ID"; "user-provided data"; "device ID"; and "modeling."[5]

- A "User-ID" is a "persistent ID[,]"[6] consisting of a unique combination of up to "256 characters[,]"that is created by website operators and "assign[ed] and consistently reassign[ed] … to [] users[,] … typically [] during login."[7]

- "User-provided data" consists of contact details such as "email, phone, name and address[,]" provided by website users, that "is [] matched with other Google data … to improve the accuracy of [] measurement data and power enhanced Analytics capabilities."[8] Although these personal details are "hash[ed],"[9] the reality is that, even in hashed form, they are traceable to individuals.[10]

- A "device ID" is a "browser-based or mobile-app-based identifier."[11] "On a website, device ID gets its value from the client ID property of the _ga cookie. In an iOS or Firebase app, device ID gets its value from the app-instance ID, which identifies a unique installation of the app."[12]

---

[5] GOOGLE, [GA4] REPORTING IDENTITIES, https://support.google.com/analytics/answer/10976610.

[6] *Id.*

[7] GOOGLE, [GA4] MEASURE ACTIVITY ACROSS PLATFORMS WITH USER-ID, https://support.google.com/analytics/answer/9213390.

[8] GOOGLE, [GA4] USER-PROVIDED DATA COLLECTION, https://support.google.com/analytics/answer/14077171.

[9] *Id.*

[10] *See*, *e.g.*, FEDERAL TRADE COMMISSION, DOES HASHING MAKE DATA "ANONYMOUS"?, https://tinyurl.com/56p3a82j ("[H]ashing is vastly overrated as an 'anonymization' technique … the casual assumption that hashing is sufficient to anonymize data is risky at best, and usually wrong."); FEDERAL TRADE COMMISSION, NO, HASHING STILL DOESN'T MAKE YOUR DATA ANONYMOUS, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous ("[H]ashes aren't 'anonymous' and can still be used to identify users, and their misuse can lead to harm. Companies should not act or claim as if hashing personal information renders it anonymized."); STEVEN ENGLEHARDT ET AL., I NEVER SIGNED UP FOR THIS! PRIVACY IMPLICATIONS OF EMAIL TRACKING, https://petsymposium.org/2018/files/papers/issue1/paper42-2018-1-source.pdf ("[H]ashing of PII, including emails, is not a meaningful privacy protection. This is folk knowledge in the security community, but bears repeating.").

[11] GOOGLE, [GA4] DEVICE ID, https://support.google.com/analytics/answer/9356035.

[12] *Id.*

- "Modeling" uses "machine learning to model the behavior of users who decline analytics cookies based on the behavior of similar users who accept analytics cookies."[13]

24. Google Analytics can also leverage "Google signals," which "associates [data] with user[s'] … Google accounts," for "users who have signed in."[14] "This association of data with these signed-in users is used to enable cross-device remarketing, and cross-device key events export to Google Ads."[15]

25. Thus, with Google Signals, "Google is able to develop a holistic view of how those users interact with an online property from multiple browsers and multiple devices. For example, [one] can see how users browse products on [a] site from a phone, and later return to complete purchases from a tablet or laptop."[16]

26. This gathered information is used for marketing and advertising. Namely, "Google signals enables[r]emarketing … Google Ads and other Google Marketing Platform advertising products can use third-party advertising identifiers enabled by Google signals to serve ads in … remarketing campaigns to Google users."[17]

27. Put simply, "[r]emarketing lets [Google's clients] re-engage users based on their behavior in [an] app or on [a] site. When users fit the behavioral profile for an audience (for example, Reached Level 9), they are added to that audience and are eligible to see ads related to that earlier behavior."[18]

---

[13] GOOGLE, [GA4] BEHAVIORAL MODELING FOR CONSENT MODE, https://support.google.com/analytics/answer/11161109.

[14] GOOGLE, [GA4] ACTIVATE GOOGLE SIGNALS FOR GOOGLE ANALYTICS PROPERTIES, https://support.google.com/analytics/answer/9445345.

[15] *Id.*

[16] *Id.*

[17] GOOGLE, [GA4] ACTIVATE GOOGLE SIGNALS FOR GOOGLE ANALYTICS PROPERTIES, https://support.google.com/analytics/answer/9445345.

[18] GOOGLE, ENABLE REMARKETING WITH GOOGLE ANALYTICS DATA, https://support.google.com/analytics/answer/9313634.

28. Gathered information is also used for analytics. Google Signals helps "[r]eport on cross-device user counts," "[r]eport and understand different groups of users based on the different device combinations they use," [r]eport on and understand [] cross-device marketing performance (e.g., channels, campaigns, etc.)," and "[u]nderstand the customer journey across devices by analyzing user-based reports (active users, funnels, pathing)."[19] In this sense, "Google signals enables[] … Google Analytics [to] collect[] additional information about demographics and interests … from users who are signed in to their Google accounts."[20]

29. Regardless of which service collects the information, Google uses the information for reports and insights associated with Google Analytics.

Real-Time Reporting

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

Acquisition Reports

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

Engagement Reports

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

Monetization Reports

- See how much revenue your site or app generates whether it's from ecommerce, subscriptions, or ads.

---

[19] *Id.*

[20] GOOGLE, [GA4] ACTIVATE GOOGLE SIGNALS FOR GOOGLE ANALYTICS PROPERTIES, https://support.google.com/analytics/answer/9445345.

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

30. Google Analytics also tracks portions of users' IP addresses for "analysis of general location trends" despite masking the full IP address of a user.[21]

31. This gathered information is used for marketing and advertising. Specifically, Google "Analytics is designed to work seamlessly with other Google solutions and partner products" and can "unlock deeper insights into [advertising] campaign performance from Google Ads, Display & Video 360, and Search Ads 360."[22]

32. Google Analytics integrates with Google Ads so that clients, like Defendant, can "[s]ee [] Ads data together with [] website and app performance data in the Google Ads reports in Analytics."[23] Google Analytics integrates with Display & Video 360 and Search Ads so that clients, like Defendant, can "[e]xport conversions created in Analytics," "create audiences that are predicted to take [certain] actions[,]" and "use them for automated bidding" in Display & Video 360 and Search Ads 360.[24]

[21] "In GA4, IP anonymization is automatically enabled by default. This means you don't have to configure anything—Google Analytics will automatically mask user IP addresses before they're processed or stored." SELINE ANALYTICS, WHAT IS IP ANONYMIZATION IN GOOGLE ANALYTICS?, https://seline.com/google-analytics-terms/ip-anonymization.

[22] GOOGLE, ANALYTICS FEATURES, https://marketingplatform.google.com/about/analytics/features/.

[23] *Id.*

[24] *Id.*

33. Gathered information is also used for analytics. With Google Analytics, clients, like Defendant, can "apply[] Google's machine learning models, … analyze [] data[,] and predict future actions people may take, like making a purchase or churning."[25]

34. In addition, Google Analytics can "automatically detect and surface actionable insights from [gathered] data like important changes, new trends, and other growth opportunities."[26] And Google can provide "[a]nswers to [marketers' q]uestions … in natural language[,] … to quickly find [] metric[s], report[s], or insights."[27] Through Google Analytics' "[u]ser [e]xploration" functions, it is even possible to "[s]elect specific groups of users and drill down deeper to understand how those users engage with [a] site or app."[28]

35. Thus, Google Analytics furnishes "a complete understanding of [] customers across devices and platforms[,] … [and] gives [] the tools[] … to understand customer journey and improve marketing ROI."[29]

36. Defendant discloses information to Google Analytics for such marketing, advertising, and analytics purposes.

2. Meta's Platform and Its Business

37. The Facebook social-media platform, owned by Meta, describes itself as a "real identity platform,"[30] meaning users are allowed only one account and must share "the name they go by in everyday life."[31] To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.[32]

---

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] GOOGLE, ANALYTICS OVERVIEW, https://marketingplatform.google.com/about/analytics/.

[30] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).

[31] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.

[32] FACEBOOK, SIGN UP, https://www.facebook.com.

38. With respect to the apps offered by Meta, substantially all of Meta's revenue is generated by selling advertising space.[33]

39. Meta sells advertising space by highlighting its ability to target users.[34] Meta can target users so effectively because it surveils user activity both on and off its sites.[35] This allows Meta to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[36] Meta compiles this information into a generalized dataset called "Core Audiences," which allows advertisers to reach precise audiences based on specified targeting types.[37]

40. Advertisers can also build "Custom Audiences."[38] Custom Audiences enables advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[39] With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverage[] information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[40] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Meta with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers or by utilizing Meta's "Business Tools."[41]

---

[33] *Id.* at 63.

[34] FACEBOOK, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, https://www.facebook.com/business/help/205029060038706.

[35] FACEBOOK, ABOUT META PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[36] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

[37] https://www.facebook.com/business/news/Core-Audiences.

[38] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494.

[39] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

[40] FACEBOOK, ABOUT LOOKALIKE AUDIENCES, https://www.facebook.com/business/help/164749007013531?id=401668390442328.

[41] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; FACEBOOK,

41. As Meta puts it, the Business Tools "help website owners and publishers, app developers, and business partners, including advertisers and others, integrate with [Facebook], understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[42] Put more succinctly, Meta's Business Tools are bits of code that advertisers can integrate into their websites, mobile applications, and servers, thereby enabling Meta to intercept and collect user activity on those platforms.

42. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[43] Meta's Business Tools can also track other events. Meta offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[44] Advertisers can even create their own tracking parameters by building a "custom event."[45]

43. One such Business Tool is the Facebook Pixel (the "Facebook Pixel"). Meta offers this piece of code to advertisers, like Defendant, to integrate into their websites. The Facebook Pixel "tracks the people and type of actions they take."[46] When a user accesses a website hosting the Facebook Pixel, Meta's software script surreptitiously directs the user's browser to contemporaneously send a separate message to Meta's servers. This secret and contemporaneous transmission contains the original GET request sent to the host website, along with additional data

---

CREATE A WEBSITE CUSTOM AUDIENCE, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.

[42] FACEBOOK, THE META BUSINESS TOOLS, https://www.facebook.com/help/331509497253087.

[43] *See* FACEBOOK, META FOR DEVELOPERS: META PIXEL, ADVANCED, https://developers.facebook.com/docs/meta-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, META FOR DEVELOPERS: MARKETING API - APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[44] FACEBOOK, SPECIFICATIONS FOR META PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142.

[45] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, META FOR DEVELOPERS: MARKETING API – APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[46] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

that the Facebook Pixel is configured to collect. This transmission is initiated by Meta code and concurrent with the communications with the host website. At relevant times, two sets of code were thus automatically run as part of the browser's attempt to load and read Defendant's Website—Defendant's own code and Facebook's embedded code.

44. Defendant chose to include the Facebook Pixel on its Website.

45. Meta's own documentation makes clear just how much tracking of private information the Facebook Pixel does. It describes the Facebook Pixel as code that Meta's business customers can put on their website to "[m]ake sure your ads are shown to the right people. ***Find … people who have visited a specific page or taken a desired action on your website***." (Emphasis added.)[47]

46. Meta instructs such business customers that:

47. Once you've set up the [Facebook] Pixel, ***the pixel will log when someone takes an action on your website***. Examples of actions include adding an item to their shopping cart or making a purchase. ***The Pixel receives these actions, or events***, which you can view on your [Facebook] Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. ***You'll also have options to reach those customers again through future Meta ads***.[48]

48. The Facebook Pixel code enables Meta not only to help Defendant with advertising to its own users outside the Website, but also to include individual users among groups targeted by ***other*** Facebook advertisers relating to the conditions about which users took actions on Defendant's Website.

[47] Meta, ABOUT META PIXEL https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Dec. 26, 2023).

[48] *Id*. (Emphasis added.)

49. Meta's Business Help Center explains:

50. Meta ***uses marketing data to show ads to people who are likely to be interested in them***. One type of marketing data is website events, which are ***actions that people take on your website***.[49]

51. In other words, Meta sells advertising space by highlighting its ability to target users.[50] Meta can target users so effectively because it surveils user activity both on and off its sites, including Facebook.[51] This allows Meta to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and connections.[52]

52. Each time Meta intercepts this activity data, it also discloses a user's personally identifiable information, including their Facebook ID ("FID"). An FID is a unique and persistent identifier that Facebook assigns to each user. With it, any ordinary person can look up the user's Facebook profile and name. Notably, while Meta can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Meta admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to any Facebook profile.

53. A user who accessed Defendant's Website while logged into Facebook transmitted what is known as a "c_user cookie" to Facebook, which contained that user's unencrypted Facebook ID.

54. When a visitor's browser had recently logged out of an account, Facebook compelled the visitor's browser to send a smaller set of cookies.

---

[49] Meta, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS https://www.facebook.com/business/help/964258670337005?id=1205376682832142 (emphasis added)

[50] Meta, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, https://www.facebook.com/business/help/205029060038706 (last visited Dec. 26, 2023).

[51] Meta, ABOUT META PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142

[52] Meta, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting

55. One such cookie was the "fr cookie" which contained, at least, an encrypted Facebook ID and browser identifier.[53] Facebook, at a minimum, used the fr cookie to identify users.[54]

56. If a visitor had never created an account, an even smaller set of cookies was transmitted.

57. At each stage, Defendant also utilized the "_fbp cookie," which attached to a browser as a first-party cookie, and which Facebook used to identify a browser and a user.[55]

58. The c_user cookie expires after 90 days if the user checked the "keep me logged in" checkbox on the website.[56] Otherwise, the c_user cookie is cleared when the browser exits.[57]

59. The The fr cookie expires after 90 days unless the visitor's browser logs back into Facebook.[58] If that happens, the time resets, and another 90 days begins to accrue.[59]

60. The _fbp cookie expires after 90 days unless the visitor's browser accesses the same website.[60] If that happens, the time resets, and another 90 days begins to accrue.[61]

61. The Facebook Pixel used both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—*i.e.*, Defendant's Website.[62] A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—*i.e.*,

---

[53] DATA PROTECTION COMMISSIONER, FACEBOOK IRELAND LTD, REPORT OF RE-AUDIT (Sept. 21, 2012), http://www.europe-v-facebook.org/ODPC_Review.pdf.

[54] FACEBOOK, PRIVACY CENTER – COOKIES POLICY, https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3.

[55] *Id.*

[56] Seralthan, FACEBOOK COOKIES ANALYSIS (Mar. 14, 2019), https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbdf8a.

[57] *Id.*

[58] *See id.*

[59] Confirmable through developer tools.

[60] FACEBOOK, PRIVACY CENTER – COOKIES POLICY, https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3.

[61] Also confirmable through developer tools.

[62] PC MAG, FIRST-PARTY COOKIE, https://www.pcmag.com/encyclopedia/term/first-party-cookie. This is confirmable by using developer tools to inspect a website's cookies and track network activity.

Facebook.[63] The _fbp cookie was always transmitted as a first-party cookie. A duplicate _fbp cookie was sometimes sent as a third-party cookie, depending on whether the browser had recently logged into Facebook.

62. Meta at a minimum, used the fr, _fbp, and c_user cookies to link to Facebook IDs and corresponding Facebook profiles. As demonstrated below, Defendant discloses these identifiers alongside the event data.

63. The Meta Pixel is designed to collect information about website visitors that can be matched to an individual's Facebook profile for the purpose of sending targeted advertising to that user.

3. The TikTok Pixel and TikTok for Business

64. TikTok offers a SaaS called "TikTok Pixel," which "helps businesses track the performance of their ads" by simultaneously sending information from the business's website to TikTok, which then uses that information to optimize ad campaigns on TikTok and across the internet.[64]

65. The TikTok Pixel can be "plugged in" to any website, as the pixel is a piece of code that can be added to any website to capture "events" (any activity by a user that happens on a website).

66. The TikTok Pixel is part of a package of prebuilt software tools under the "TikTok for Business" product line that allow the delivery of personalized ads. By employing TikTok to collect user information through the TikTok Pixel, websites that procure TikTok's services can use the information to deliver more effective targeted advertisements, increasing revenue for the websites.

67. In short, when users interact with a webpage with the TikTok Pixel installed, the TikTok Pixel collects the "Metadata and button clicks" (information about what the user clicked on—such as the specific URL address visited by the user— or text entered into the webpage), a

[63] PC MAG, THIRD-PARTY COOKIE, https://www.pcmag.com/encyclopedia/term/third-party-cookie. This is also confirmable by tracking network activity.

[64] "TikTok Pixel 101: What It Is & How to Use It," https://popupsmart.com/blog/tiktok-pixel.

timestamp for the event, and the visitor's IP address.[65] That information is automatically and simultaneously sent to TikTok.

68. The "TikTok for Business" business model involves entering into voluntary partnerships with various companies and surveilling communications on their partners' websites with the TikTok Pixel.

69. Thus, through websites that employ TikTok's services, TikTok directly receives the electronic communications that website visitors enter into search bars, chat boxes, and button selections in real time.

70. When the TikTok Pixel is used on a website, it is not like a tape recorder or a "tool" used by one party to record the other. Instead, the TikTok Pixel involves TikTok, a separate and distinct third-party entity from the parties in the conversation, using the TikTok Pixel to eavesdrop on, record, extract information from, and analyze a conversation to which it is not a party. This is so because TikTok itself is collecting the content of any conversation. That information is then analyzed by TikTok before being provided to any entity that was a party to the conversation (like Defendant).

71. Once TikTok intercepts website communications, it has the capability to use such information for its own purposes. TikTok's Commercial Terms of Service grant TikTok "a non-exclusive, royalty-free, worldwide, transferable, sublicensable license to access, use, host, cache, store, display, publish, distribute, modify and adapt [information collected from partner websites] in order to develop, research, provide, promote, and improve TikTok's products and services."[66]

72. In practice, this means the information collected is used to: (i) analyze trends in consumer behavior based on data collected from websites across the internet that TikTok can then use when providing targeted advertising to other companies; (ii) create consumer profiles of specific users, allowing TikTok to sell future customers targeted advertising to consumers with

[65] "About TikTok Pixel," https://ads.tiktok.com/help/article/tiktok-pixel?redirected=2.

[66] "TikTok For Business Commercial Terms Of Service" https://ads.tiktok.com/i18n/official/policy/commercial-terms-of-service.

specific profile characteristics; and (iii) develop new TikTok Business products and services, or improve pre-existing TikTok Business products and services

D. Defendant discloses Grok Users' Full Conversations With Grok and PII to the Third Parties

1. Defendant discloses Grok Users' Full Conversations With Grok and PII to Google

73. When a user enters information into Grok, Defendant discloses that information to Google in real time.

74. A recent report, titled "Your AI Assistant Is Leaking Your Conversations" found that several of the most widely used AI Chatbots, including Grok, were sharing information about users' queries with third parties.[67]

75. The report found that when users engage in conversations with Grok, Defendant conspires with Google to intercept the full transcript of the users' conversations by sharing the conversation URL, along with the page title and identifying metadata. Notably, these interceptions occur regardless of what users choose in regards to cookies on the Website.

76. Defendant also transmits the Secure-3PSID cookie, which contains the user's Google profile ID, along with several other Google Signal cookies.

77. Transmissions from users' browsers to Google occur in the same manner on each website where the technology is loaded. When an action is taken on a website, the individual's browser sends a GET request to Defendant's server requesting that server to load the particular webpage. Google's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, without alerting the individual that this is happening. The Pixel, installed by Defendant causes the browser to secretly and contemporaneously duplicate the communication

[67] Your AI Assistant Is Leaking Your Conversations, LeakyLM, https://leakylm.github.io/#leakage-matrix.

with a website transmitting it to Google's servers, alongside additional information that transcribes the communication's content and the individual's identity. This transmission is initiated by Google's code and concurrent with the communications with the host website.

78. Google receives each conversation via Google Analytics and immediately views the information contained therein, processes it, and adds it to datasets to target advertisements in the manner described above.

2. Defendant discloses Grok Users' Full Conversations With Grok and PII to Meta

79. When a user enters information into Grok, Defendant discloses that information to Meta in real time.

80. The report found that when users engage in conversations with Grok, Defendant conspires with Meta to intercept the full transcript of the users' conversations by sharing the conversation URL, along with the page title.

81. Defendant also transmits the fbp cookie, which contains the user's Facebook profile ID, along with other cookies.

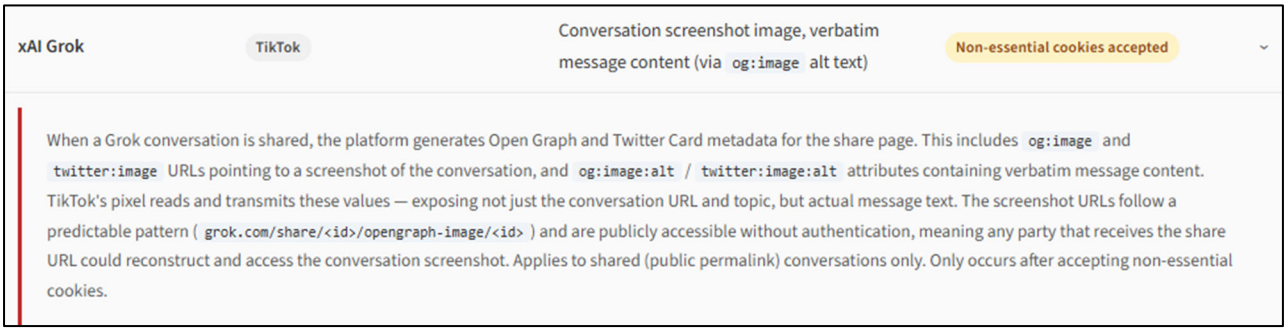
82. Transmissions from users' browsers to Meta occur in the same manner on each website where the technology is loaded. When an action is taken on a website, the individual's browser sends a GET request to Defendant's server requesting that server to load the particular webpage. Meta's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, without alerting the individual that this is happening. The Pixel, installed by Defendant causes the browser to secretly and contemporaneously duplicate the communication with a website transmitting it to Meta's servers, alongside additional information that transcribes the communication's content and the individual's identity. This transmission is initiated by Meta's code and concurrent with the communications with the host website.

83. Meta receives each conversation via the Facebook Pixel and immediately views the information contained therein, processes it, and adds it to datasets to target advertisements in the manner described above.

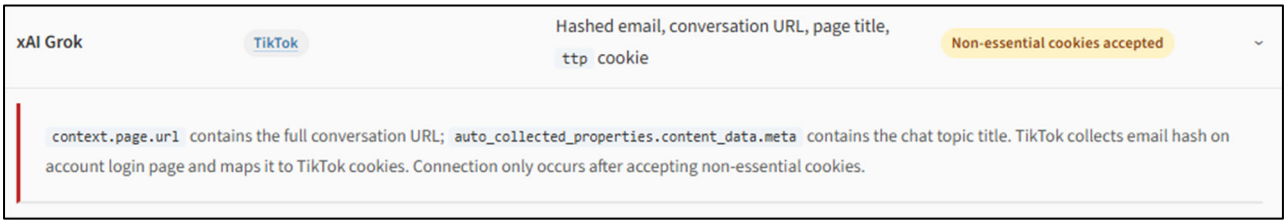
3. Defendant discloses Grok Users' Full Conversations With Grok and PII to TikTok

84. When a user enters information into Grok, Defendant discloses that information to TikTok in real time.

85. The report found that when users engage in conversations with Grok, Defendant conspires with TikTok to intercept a full transcript of the users' conversations, the conversation URL, along with the page title.



86. Defendant also transmits a "hashed" version of the users' email address to TikTok, identifying the user and associating them with the transcript.



87. The TikTok Pixel is designed to collect information about website visitors that can be matched to an individual's existing profile for the purpose of sending targeted advertising to that user. Though AdTech companies claim "hashing" would prevent a party that is not TikTok from obtaining the subscriber's email address, TikTok, as the recipient of the data and the entity that

creates the hash, can decrypt the hashed email addresses it receives and match it to its existing advertising profiles.

88. Transmissions from users' browsers to TikTok occur in the same manner on each website where the technology is loaded. When an action is taken on a website, the individual's browser sends a GET request to Defendant's server requesting that server to load the particular webpage. TikTok's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, without alerting the individual that this is happening. The Pixel, installed by Defendant causes the browser to secretly and contemporaneously duplicate the communication with a website transmitting it to TikTok's servers, alongside additional information that transcribes the communication's content and the individual's identity. This transmission is initiated by TikTok's code and concurrent with the communications with the host website.

89. TikTok receives each conversation via the TikTok Pixel and immediately views the information contained therein, processes it, and adds it to datasets to target advertisements in the manner described above.

CLASS ALLEGATIONS

90. **Class Definition:** Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of himself and other similarly situated individuals defined as all persons who, during the class period, had their personally identifiable information and communications with Grok disclosed to third party entities, as a result of using the Website (the "Class").

91. **California Subclass:** Plaintiff also brings this action on behalf of himself and other similarly situated individuals defined as all California residents who, during the class period, had their personally identifiable information and communications with Grok disclosed to third party entities, as a result of using the Website while in California (the "California Subclass").

92. Plaintiff reserves the right to modify the class or subclass definition or add sub-classes as necessary prior to filing a motion for class certification.

93. Excluded from the Class is Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer director, or

employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

94. Numerosity/Ascertainability. Members of the Class are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiff at this time; however, it is estimated that there are millions of individuals in the Class. The identity of such membership is readily ascertainable from Defendant's records and non-party records, such as those of Google.

95. Typicality. Plaintiff's claims are typical of the claims of the Class because Plaintiff used the Website and, as a result of Defendant's unlawful conduct, had their PII and communications intercepted by third parties without their express written authorization or knowledge. Plaintiff's claims are based on the same legal theories as the claims of other Class Members.

96. Adequacy. Plaintiff is fully prepared to take all necessary steps to represent fairly and adequately the interests of the Class Members. Plaintiff's interests are coincident with, and not antagonistic to, those of the members of the Class. Plaintiff is represented by attorneys with experience in the prosecution of class action litigation generally and in the emerging field of digital privacy litigation specifically. Plaintiff's attorneys are committed to vigorously prosecuting this action on behalf of the members of the Class.

97. Common Questions of Law and Fact Predominate/Well Defined Community of Interest. Questions of law and fact common to the members of the Class predominate over questions that may affect only individual members of the Class because Defendant has acted on grounds generally applicable to the Class. Such generally applicable conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the Class includes:

(a) Whether Defendant intentionally installed wiretaps into the code of its Website;

(b) Whether Defendant's Website contains code that permits third parties, such as Google, Meta, and TikTok, to intercept users' PII, and related communications;

(c) Whether Google, Meta, and TikTok are third-party eavesdroppers;

(d) Whether Plaintiff's and Class Members' communications via the Website and the resultant interceptions thereof constitute an affirmative act of communication;

(e) Whether Defendant's conduct, which allowed the Third Parties—unauthorized persons—to view Plaintiff's and Class Members' PII and communications, resulted in a breach of confidentiality;

(f) Whether Defendant violated Plaintiff's and Class Members' privacy rights by using third-party technology, such as Google Analytics, the Facebook Pixel, and the TikTok Pixel, to allow third parties to intercept users' online communications along with information that uniquely identified him;

(g) Whether Plaintiff and Class Members are entitled to damages under the ECPA, CIPA, or any other relevant statute; and

(h) Whether Defendant's actions violate Plaintiff's and Class Members' privacy rights as provided by the California Constitution and common law.

98. Superiority. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiff knows of no special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

COUNT I
Violation of the Electronic Communications Privacy Act,
18 U.S.C. § 2511, *et seq.*

99. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

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

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

102. The ECPA protects both sending and the receipt of communications.

103. 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.

104. The transmission of Plaintiff's PII and communications to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

105. The transmission of PII and sensitive information between Plaintiff 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(12).

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

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

108. 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).

109. The following instruments constitute "devices" within the meaning of the ECPA:

a. The computer codes and programs Defendant and the Third Parties used to track Plaintiff and Class Members' communications while they were navigating the Website;

b. Plaintiff's and Class Members' browsers;

c. Plaintiff's and Class Members' mobile devices;

d. Defendant's and Third Parties' web and ad servers;

e. The plan the Defendant and third parties carried out to effectuate the tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser to navigate the Website.

110. Plaintiff and Class Members' interactions with Defendant's Website are electronic communications under the ECPA.

111. By utilizing and embedding the tracking technology provided by the Third Parties on its Website, Defendant intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiff and Class Members in violation of 18 U.S.C. § 2511(1)(a).

112. Specifically, Defendant intercepted—in real time—Plaintiff's and Class Members' electronic communications via the tracking technology provided by Google on the Website, which tracked, stored and unlawfully disclosed Plaintiff's and Class Members' PII and communications to Third Parties.

113. Defendant intercepted communications that include, but are not necessarily limited to, communications to/from Plaintiff and Class Members regarding PII, including their identities and specific queries and conversations they entered into Grok. This confidential information is then monetized for targeted advertising purposes, among other things.

114. By intentionally disclosing or endeavoring to disclose Plaintiff's and Class Members' electronic communications to the 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).

115. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class members' electronic communications, 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).

116. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States or of any state, namely, CIPA and invasion of privacy, among others.

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

118. Defendant was not acting under the color of law to intercept Plaintiff and Class members' wire or electronic communications.

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

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

121. As a result of each and every violation thereof, on behalf of himself and the Class, Plaintiff seeks statutory damages of $10,000 or $100 per day for each violation of 18 U.S.C. §§ 2510, *et seq*.

COUNT II
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 631

122. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the California Subclass.

123. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. CIPA begins with its statement of purpose – namely, that the purpose of CIPA is to "protect the right of privacy of the people of [California]" from the threat posed by "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications . . . ." Cal. Penal Code § 630.

124. A person violates California Penal Code § 631(a), if:

> by means of any machine, instrument, or contrivance, or in any other manner, [s/he] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [s/he] willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [s/he] uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained . . . .

Cal. Penal Code § 631(a).

125. Further, a person violates § 631(a) if s/he "aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned" in the preceding paragraph. *Id.*

126. To avoid liability under § 631(a), a defendant must show it had the consent of <u>all</u>

parties to a communication.

127. At all relevant times, Defendant aided, agreed with, and conspired with Google to track and intercept Plaintiff's and Class Members' internet communications while using the Website. These communications were intercepted without the authorization and consent of Plaintiff and Class Members.

128. Defendant, when aiding and assisting the wiretapping, which occurred in California, intended to help Google learn some meaning of the content of users' queries to Grok.

129. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, Google Analytics falls under the broad catch-all category of "any other manner":

a. The computer codes and programs the Third Parties used to track Plaintiff's and Class Members' communications while they were using Grok;

b. Plaintiff's and Class Members' browsers;

c. Plaintiff's and Class Members' computing and mobile devices;

d. Google's, Meta's, and TikTok's web and ad servers;

e. The web and ad-servers from which the Third Parties tracked and intercepted Plaintiff's and Class Members' communications while they were using a web browser to use Grok;

f. The computer codes and programs used by Google to effectuate the tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit the Website; and

g. The plan Defendant and each Third Party carried out to effectuate tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser to use the Website.

130. As demonstrated hereinabove, Defendant violated CIPA by aiding and permitting third parties to receive its users' online communications through the Website without their consent.

131. As a result of the above violations, Defendant is liable to Plaintiff and other California Subclass Members in the amount of, the greater of, $5,000 dollars per violation or three

times the amount of actual damages. Additionally, Cal. Penal Code § 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages."

COUNT III
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 632

132. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the California Subclass.

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

134. Section 632 defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto[.]"

135. Plaintiff's and Class members' communications to Defendant, including their sensitive personal, financial, medical, and other information, were confidential communications for purposes of § 632, because Plaintiff and Class Members had an objectively reasonable expectation of privacy in this data.

136. Plaintiff and Class Members expected their communications to be confined to Defendant in part, due to the protected nature of the information at issue. Plaintiff and Class Members did not expect the Third Parties secretly eavesdrop upon or record this confidential information and their communications.

137. The Third Parties' tracking technology are each an electronic amplifying or recording devices for purposes of § 632.

138. By contemporaneously intercepting and recording Plaintiff's and Class Members' confidential communications to Defendant through this technology, the Third Parties eavesdropped

and/or recorded confidential communications through an electronic amplifying or recording device in violation of § 632 of CIPA.

139. At no time did Plaintiff or Class Members consent to the Defendant's conduct, nor could they reasonably expect that their communications would be overheard or recorded by the Third Parties.

140. Each Third Party utilized Plaintiff's and Class Members' sensitive personal information for its own purposes, including for targeted advertising.

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

142. Plaintiff and California Subclass Members have also suffered irreparable injury from these unauthorized acts. Plaintiff's and California Subclass Members' sensitive data has been collected, viewed, accessed, stored, by Google, have not been destroyed, and due to the continuing threat of such injury, have no adequate remedy at law. Plaintiff and California Subclass Members are accordingly entitled to injunctive relief.

COUNT IV
Invasion of Privacy Under California's Constitution/Intrusion Upon Seclusion

143. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the members of the Class.

144. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health 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 wiretaps without Plaintiff's and Class Members' knowledge or consent.

145. At all relevant times, by using Google Analytics, the Facebook Pixel, and the TikTok Pixel to record and communicate users' identifying information, alongside their

confidential communications, Defendant intentionally invaded Plaintiff's and Class Members' privacy rights under the California Constitution, as well as intruded upon Plaintiff's and Class Members' seclusion.

146. Plaintiff and Class Members had a reasonable expectation that their communications, identities, health information, and other data would remain confidential, and that Defendant would not install wiretaps on the Website.

147. Plaintiff and Class Members did not authorize Defendant to record and transmit Plaintiff's and Class Members' private communications alongside their personally identifiable information.

148. This invasion of privacy was serious in nature, scope, and impact because it related to patients' private communications. Moreover, it constituted an egregious breach of the societal norms underlying the privacy right.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as the representative of the Class, and Plaintiff's attorneys as Class Counsel to represent the Class Members.

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

D. For an award of damages, including, but not limited to, actual, consequential, statutory, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: May 14, 2026

BURSOR & FISHER, P.A.

By: */s/ Philip L. Fraietta*
Philip L. Fraietta

Philip L. Fraietta (State Bar No. 354768)
50 Main Street, Suite 475
White Plains, NY 10606
Telephone: (914) 874-0708
Facsimile: (914) 206-3656
E-mail: pfraietta@bursor.com

BURSOR & FISHER, P.A.
Max S. Roberts (State Bar No. 363482)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: mroberts@bursor.com

BURSOR & FISHER, P.A.
Joshua R. Wilner (State Bar No. 353949)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: jwilner@bursor.com

Attorneys for Plaintiff

ClassAction.org
