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
E-mail: jwilner@bursor.com

Attorney for Plaintiff

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

STEPHEN JAMES, individually and on behalf of all others similarly situated,

Plaintiff,

v.

KALSHI, INC.,

Defendant.

Case No.: '26CV3556 RSH DDL

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Stephen James ("Plaintiff"), individually and on behalf of all other persons similarly situated, by and through his attorneys, makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to allegations specifically pertaining to himself and his counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action lawsuit brought on behalf of all persons who have accessed and used www.kalshi.com (the "Website") to place a trade or wager.

2. Defendant offers a platform to bet on nearly any event imaginable, including political races, sports games, crypto markets, and even climate change, through its Website. Consumers must provide a dollar amount and interact with Defendant's website to place a bet on a specific outcome. When consumers provide this information to Defendant, they expect that such confidential information and activity will be protected and not disclosed to unknown third parties. Such expectations are based, in part, on the legal protections afforded to such information.

3. Despite reasonable expectations of privacy, and Defendant's legal duties to prevent the disclosure of such private information, Defendant disclosed information regarding each bet made on the Website to Google, LLC (Google) and LinkedIn Corporation ("LinkedIn") (together, the "Third Parties"). These disclosures include communications that contain sensitive and confidential information.

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

THE PARTIES

5. Plaintiff Stephen James is a citizen of California, residing in Chula Vista, California. Plaintiff has placed numerous bets on the website in 2026, including as recently as March, 2026.

6. Plaintiff entered personal information and information regarding each bet into the Website using the same device and browser used to access his LinkedIn account.

7. Unbeknownst to Plaintiff, Defendant disclosed his personally identifiable information ("PII") to Google and LinkedIn. Neither Defendant, nor either Third Party, procured Plaintiff's prior consent to the sharing of his private and protected information.

8. Defendant Kalshi, Inc. is a Delaware corporation with its principal place of business at 594 Broadway Room 407, New York, NY 10012. Defendant develops, owns, and operates the Website, which is available throughout the United States.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under a law of the United States (the Electronic Communications Privacy Act, 18 U.S.C. § 2511). This Court also has supplemental jurisdiction over Plaintiff's state law claims under 28 U.S.C. § 1367. Further, this action is a putative class action, and Plaintiff alleges that at least 100 people comprise the proposed class, that the combined claims of the proposed class members exceed $5,000,000 exclusive of interest and costs, and that at least one member of the proposed class is a citizen of a state different from the defendant.

10. This Court has personal jurisdiction over the parties because Plaintiff resides in California, is a California citizen, and submits to the jurisdiction of the Court. Further, the Defendant has, at all times relevant hereto, systematically and continually conducted business in California, including within this District, and intentionally availed itself of the benefits and privileges of the California consumer market through the promotion, marketing, and operation of its services to residents within this District and throughout California. Additionally, Plaintiff, while in California, placed bets through Defendant's Website.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because the Defendant transacts significant business within this District and the acts that gave rise to this cause of action occurred within this District. Further, Plaintiff resides in this District.

FACTUAL ALLEGATIONS

I. THE CALIFORNIA INVASION OF PRIVACY ACT

12. The California Legislature enacted the Invasion of Privacy Act to protect certain privacy rights of California citizens. The legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

13. The California Supreme Court has repeatedly stated an "express objective" of CIPA is to "protect a person placing or receiving a call from a situation where the person on the other end of the line *permits an outsider to tap his telephone or listen in on the call*." *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985) (emphasis added).

14. Further, as the California Supreme Court has held in explaining the legislative purpose behind CIPA:

> While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its *simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device.*
>
> As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements.

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

15. As part of CIPA, the California Legislature enacted § 631(a), which prohibits any person or entity from [i] "intentionally tap[ping], or mak[ing] any unauthorized connection … with any telegraph or telephone wire," [ii] "willfully and without the consent of all parties to the communication … read[ing], or attempt[ing] to read, or to learn the contents or meaning of any . . . 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]," or [iii] "us[ing], or attempt[ing] to use . . . any information so obtained."

16. CIPA § 631(a) also penalizes those who "aid[], agree[] with, employ[], or conspire[] with any person" who conducts the aforementioned wiretapping, or those who "permit" the wiretapping.

17. As part of the Invasion of Privacy Act, the California Legislature additionally introduced Penal Code § 632(a), which prohibits any person or entity from "intentionally and without the consent of all parties to a confidential communication, us[ing] an electronic amplifying or recording device to eavesdrop upon or record [a] confidential communication."

18. A "confidential communication" for the purposes of CIPA § 632 is "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." Cal. Penal Code § 632(c).

19. Individuals may bring an action against the violator of CIPA §§ 631 and 632 for $5,000 per violation. Cal. Penal Code § 637.2(a)(1).

III. DEFENDANT DISCLOSES USERS' PRIVATE INFORMATION TO LINKEDIN AND GOOGLE

A. LinkedIn's Platform and Business Tools

20. LinkedIn markets itself as "the world's largest professional network on the internet[.]"[1] But LinkedIn is no longer simply a tool to help users find jobs or expand their professional network. LinkedIn has moved into the marketing and advertising space, and boasts of its ability to allow potential advertisers to "[r]each 1 billion+ professionals around the world" via its Marketing Solutions services.[2] Recently, LinkedIn was projected as being responsible for "roughly 0.9 percent of the global ad revenue" which included approximately $5.91 billion in advertising revenue in 2022.[3]

21. According to LinkedIn, "[t]argeting is a foundational element of running a successful advertising campaign — [g]etting your targeting right leads to higher engagement, and ultimately, higher conversion rates." [4] Targeting refers to ensuring that advertisements are targeted to, and appear in front of, the target demographic for an advertisement. To that end, LinkedIn's Marketing Solutions services allow potential advertisers to "[b]uild strategic campaigns" targeting specific users.[5] LinkedIn's "marketing solutions allow advertisers to select specific characteristics to

---

[1] LINKEDIN, WHAT IS LINKEDIN AND HOW CAN I USE IT?, https://www.linkedin.com/help/linkedin/answer/a548441#.

[2] LINKEDIN, MARKETING SOLUTIONS, https://business.linkedin.com/marketing-solutions.

[3] Valentina Dencheva, *LinkedIn annual ad revenue 2017-2027*, STATISTA (Dec. 12, 2023), https://www.statista.com/statistics/275933/linkedins-advertising-revenue.

[4] LINKEDIN, REACH YOUR AUDIENCE: TARGETING ON LINKEDIN, p.3, https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/resources/pdfs/linkedin-targeting-playbook-v3.pdf.

[5] LINKEDIN, *supra* note 33.

help them reach their ideal audience. The ads [users] see on LinkedIn are then targeted to provide content relevant to [the users]."[6]

22. As a result of its activities and operation of the LinkedIn Insight Tag, LinkedIn is able to make extremely personal inferences about individuals' demographics, intent, behavior, engagement, interests, buying decisions, and more.[7]

23. The personal information and communications obtained by LinkedIn are used to fuel various services offered via LinkedIn's Marketing Solutions including Ad Targeting, Matched Audiences, Audience Expansion, and LinkedIn Audience Network.[8]

24. Such information is extremely valuable to marketers and advertisers because the inferences derived from users' personal information and communications allow marketers and advertisers, including providers of financial products and services, to target potential customers.[9]

25. For example, through the use of LinkedIn's Audience Network, marketers and advertisers are able to expand their reach and advertise on sites other than LinkedIn to "reach millions of professionals across multiple touchpoints."[10] According to Broc Munro of Microsoft, "[w]e gravitate towards social platforms like

---

[6] LINKEDIN, LINKEDIN ADS AND MARKETING SOLUTIONS, https://www.linkedin.com/help/lms/answer/a421454.

[7] *See* LINKEDIN, MARKETING SOLUTIONS, https://business.linkedin.com/marketing-solutions/audience ("Target audiences through demographic marketing[,]" "Zero in on intent, behavior, engagement, interests, and more[,]" and "Reach the LinkedIn audience involved in the buying decision").

[8] *See id.*

[9] LINKEDIN, PRIVACY POLICY, https://www.linkedin.com/legal/privacy-policy ("We serve you tailored ads both on and off our Services. We offer you choices regarding personalized ads, but you cannot opt-out of seeing other ads."); LINKEDIN, ACCOUNT TARGETING, https://business.linkedin.com/marketing-solutions/ad-targeting ("Target your ideal customer based on traits like their job title, company name or industry, and by professional or personal interests").

[10] LINKEDIN, ACCOUNT TARGETING, https://business.linkedin.com/marketing-solutions/ad-targeting.

LinkedIn to achieve more targeted marketing engagement. However, we know that our audiences don't spend all their time on social media. LinkedIn Audience Network enables us to expand our reach to trusted sites while still respecting our audience targeting. This increases the impact of our advertising."[11]

26. In July 2022, "LinkedIn Marketing Solutions surpassed $5 billion in annual revenue[.]"[12] That figure is "expected to further grow to reach 10.35 billion U.S. dollars by 2027."[13]

27. According to LinkedIn, the LinkedIn Insight Tag, also called the Insight Tag is "[a] simple code snippet added to [a] website [that] can help you optimize your campaigns, retarget your website visitors, and learn more about your audiences."[14] LinkedIn represents that the LinkedIn Insight Tag "enable[s] in-depth campaign reporting and unlock[s] valuable insights about your website visitors."[15]

28. LinkedIn's current iteration of its Insight Tag is a JavaScript-based code which allows for the installation of its software.[16] A critical feature allows the LinkedIn Insight Tag to track users, even when third-party cookies are blocked.[17] LinkedIn "recommend[s] using the JavaScript-based Insight Tag or Conversions API"

---

[11] LINKEDIN, LINKEDIN AUDIENCE NETWORK, https://business.linkedin.com/marketing-solutions/native-advertising/linkedin-audience-network.

[12] *LinkedIn Business Highlights from Microsoft's FY22 Q4 Earnings*, LINKEDIN PRESSROOM (July 25, 2022), https://news.linkedin.com/2022/july/linkedin-business-highlights-from-microsoft-s-fy22-q4earnings#:~:text=And%20LinkedIn%20Marketing%20Solutions%20surpassed,revenue%20for%20the%20first%20time.

[13] Dencheva, *supra* note 34.

[14] LINKEDIN, INSIGHT TAG, https://business.linkedin.com/marketing-solutions/insight-tag.

[15] LINKEDIN, LINKEDIN INSIGHT TAG FAQS, https://www.linkedin.com/help/lms/answer/a427660.

[16] LINKEDIN, *supra* note 45.

[17] *Id.* ("It's important for advertisers to prepare for these changes by switching to JavaScript tags and enabling 'enhanced conversion tracking' in the Insight Tag settings to continue capturing signals where 3rd party cookies are blocked.").

because third-party cookie settings are being deprecated across the industry.[18] Embedding the JavaScript as a first-party cookie causes users' browsers to treat the LinkedIn Insight Tag as though it is offered by the website being visited, rather than by LinkedIn. Doing so ensures that the third-party cookie-blocking functions of modern web browsers do not prevent LinkedIn from collecting data through its Pixel.[19] Instead, the LinkedIn Pixel is shielded with the same privacy exemptions offered to first-party cookies.

29. When a user who has signed in to LinkedIn (even if the user subsequently logs out) is browsing a website where the LinkedIn Insight Tag has been embedded, an HTTP request is sent using cookies, which includes information about the user's actions on the website.

30. These cookies also include data that differentiate users from one another and can be used to link the data collected to the user's LinkedIn profile.

31. The HTTP request about an individual who has previously signed into LinkedIn includes requests from the "li_sugr" and "lms_ads" cookies. Each of these cookies are used by LinkedIn "to identify LinkedIn Members off LinkedIn" for advertising purposes.[20]

32. For example, the "li_sugr" cookie is "[u]sed to make a probabilistic match of a user's identity."[21] Similarly, the "lms_ads" cookie is "[u]sed to identify LinkedIn Members off LinkedIn for advertising."[22]

33. A LinkedIn profile contains information including an individual's first and last name, place of work, contact information, and other personal details. Based

---

[18] *See id.*

[19] *See id.*

[20] LINKEDIN, LINKEDIN COOKIE TABLE, https://www.linkedin.com/legal/l/cookie-table.

[21] *See id.*

[22] *See id.*

on information it obtains through the LinkedIn Insight Tag, LinkedIn targets its account holders for advertising.

34. LinkedIn never receives consent from users to intercept and collect electronic communications containing their sensitive and unlawfully-disclosed information. In fact, LinkedIn expressly warrants the opposite.

35. When first signing up, a user agrees to the User Agreement.[23] By using or continuing to use LinkedIn's Services, users agree to two additional agreements: the Privacy Policy[24] and the Cookie Policy.[25] For California residents, LinkedIn also publishes a California Privacy Disclosure.[26]

36. LinkedIn's Privacy Policy begins by stating that "LinkedIn's mission is to connect the world's professionals . . . . Central to this mission is our commitment to be transparent about the data we collect about you, how it is used and with whom it is shared."[27]

37. The Privacy Policy goes on to describe what data LinkedIn collects from various sources, including cookies and similar technologies.[28] LinkedIn states "we use cookies and similar technologies (e.g., pixels and ad tags) to collect data (e.g., device IDs) to recognize you and your device(s) on, off and across different services and devices where you have engaged with our Services. We also allow some others to use cookies as described in our Cookie Policy."[29]

---

[23] LINKEDIN, USER AGREEMENT, https://www.linkedin.com/legal/user-agreement.

[24] LINKEDIN, PRIVACY POLICY, https://www.linkedin.com/legal/privacy-policy.

[25] LINKEDIN, COOKIE POLICY, https://www.linkedin.com/legal/cookie-policy.

[26] LINKEDIN, CALIFORNIA PRIVACY DISCLOSURE, https://www.linkedin.com/legal/california-privacy-disclosure.

[27] LINKEDIN, PRIVACY POLICY, https://www.linkedin.com/legal/privacy-policy.

[28] *Id.*

[29] *Id.*

38. However, LinkedIn offers an express representation: "**We will only collect and process personal data about you where we have lawful bases.**"[30]

39. Despite this explicit representation, Defendant unlawfully disclosed sensitive and protected information to LinkedIn in violation of state and federal privacy laws.

40. Users never choose to provide sensitive information to LinkedIn because, among other reasons, they never know whether a particular website uses the LinkedIn Insight Tag, and, if so, what sensitive personal data it collects or receives.

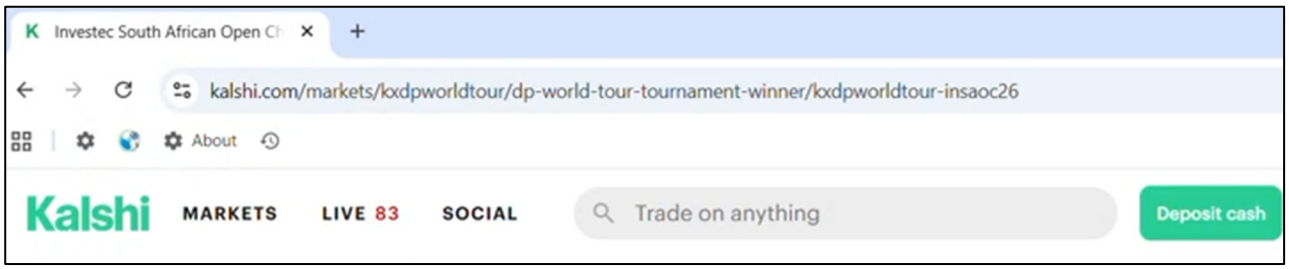
B. How Defendant Disclosed Plaintiff's and Class Members' Protected Personally Identifiable Information and Communications Through The LinkedIn Insight Tag

41. Kalshi owns and operates the Website, where it encourages visitors to make specific trades .

42. At all relevant times, Defendant's Website utilized the LinkedIn Insight Tag.

43. Through the LinkedIn Insight Tag, Defendant disclosed its customers' identities and online activity, including information related to the wagers they placed and the pages they selected.

44. When a user selects a specific event on which to place a wager, LinkedIn intercepts the detailed URL disclosing the selection made by the user.



[30] *Id.* (emphasis added).

```
"domain": "kalshi.com",
"url":
"https://kalshi.com/markets/kxdpworldtour/dp-world-tour-tournament-winner/kxdpworldtour-insaoc26",
"pageTitle": "Investec South African Open Championship Winner? Odds & Predictions 2026",
"websiteSignalRequestId": "4c4409e9-1ac0-1b46-b405-3eb40fdc1a8f",
"isTranslated": false,
"liFatId": "",
"liGiant": "",
"misc": {
  "psbState": -4
},
"isLinkedInApp": false,
```


45. Similarly, when the user selects "buy" and places a wager, LinkedIn intercepts that communication with the website via a "click" event.


```
"domain": "kalshi.com",
"url":
"https://kalshi.com/markets/kxdpworldtour/dp-world-tour-tournament-winner/kxdpworldtour-insaoc26",
"pageTitle": "Investec South African Open Championship Winner? Odds & Predictions 2026",
"websiteSignalRequestId": "4c4409e9-1ac0-1b46-b405-3eb40fdc1a8f",
"isTranslated": false,
"liFatId": "",
"liGiant": "",
"misc": {
  "psbState": -4
},
"isLinkedInApp": false,
"hem": null,
"signalType": "CLICK",
"href": "",
"domAttributes": {
  "elementSemanticType": null,
  "elementValue": null,
  "elementType": "button",
  "tagName": "BUTTON",
  "backgroundImageSrc": null,
  "imageSrc": null,
  "imageAlt": null,
  "innerText": "Buy",
```


46. LinkedIn also collects identifying cookies, including the li_sugar cookie, in the manner described above.

47. Transmissions from users' browsers to LinkedIn 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. LinkedIn'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 LinkedIn's servers, alongside additional information that transcribes the communication's content and the individual's identity. This transmission is initiated by LinkedIn's code and concurrent with the communications with the host website

48. The information disclosed by Defendant allows LinkedIn to know the identities of specific individuals as well as their private financial information. This allows these companies, including Defendant, to profit from this information for targeted advertising purposes.

49. When users place wagers on the website, they expect this information to be kept confidential.

50. Through the above-listed LinkedIn tracking services, which Defendant used via the software code installed, integrated and embedded into the Website, Defendant disclosed its customers' legally protected information.

51. Defendant engages in this deceptive conduct for its own profit at the expense of its customers' privacy. Such disclosures are an invasion of privacy, lead to harassing targeted advertising, and violate federal and state law.

C. Google Analytics' Tracking Code

52. "Google Analytics is a platform that collects data from [] websites and apps to create reports that provide insights into [] business[es]."[31]

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

53. To discern when "two different [users] interact with [a] website[,] … Google Analytics identifies an individual user based on [Google Analytics] reporting identit[ies.]"[32] Reporting identities are combinations of "identifiers … called *identity spaces*"—namely, "User-ID"; "user-provided data"; "device ID"; and "modeling."[33]

- A "User-ID" is a "persistent ID[,]"[34] 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."[35]

- "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."[36] Although these personal details are "hash[ed],"[37] the reality is that, even in hashed form, they are traceable to individuals.[38]

---

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

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

[34] *Id.*

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

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

[37] *Id.*

[38] *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 "device ID" is a "browser-based or mobile-app-based identifier."[39] "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."[40]

- "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."[41]

54. Google Analytics can also leverage "Google signals," which "associates [data] with user[s'] … Google accounts," for "users who have signed in."[42] "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."[43]

55. 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."[44]

56. This gathered information is used for marketing and advertising. Namely, "Google signals enables[r]emarketing … Google Ads and other Google Marketing

---

a meaningful privacy protection. This is folk knowledge in the security community, but bears repeating.").

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

[40] *Id.*

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

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

[43] *Id.*

[44] *Id.*

Platform advertising products can use third-party advertising identifiers enabled by Google signals to serve ads in … remarketing campaigns to Google users."[45]

57. 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."[46]

58. 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)."[47] 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."[48]

59. 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

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

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

[47] *Id.*

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

sources.

- Traffic Acquisition[:] See a session-based view of traffic and engagement on your site or app through different paid and organic traffic sources.

Engagement Reports

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

Monetization Reports

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

60. Google Analytics also tracks portions of users' IP addresses for "analysis of general location trends" despite masking the full IP address of a user.[49]

[49] "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

61. 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."[50]

62. 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."[51] 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.[52]

63. 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."[53]

64. In addition, Google Analytics can "automatically detect and surface actionable insights from [gathered] data like important changes, new trends, and other growth opportunities."[54] And Google can provide "[a]nswers to [marketers' q]uestions … in natural language[,] … to quickly find [] metric[s], report[s], or insights."[55] Through Google Analytics' "[u]ser [e]xploration" functions, it is even possible to

---

ANONYMIZATION IN GOOGLE ANALYTICS?, https://seline.com/google-analytics-terms/ip-anonymization.

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

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] *Id.*

"[s]elect specific groups of users and drill down deeper to understand how those users engage with [a] site or app."[56]

65. 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."[57]

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

D. How Defendant Disclosed Plaintiff's and Class Members' Protected Personally Identifiable Information and Communications Through Google Analytics

67. At all relevant times, Defendant's Website utilized Google Analytics.

68. Through Google Analytics, Defendant disclosed its customers' identities and online activity, including information related to the pages they selected.

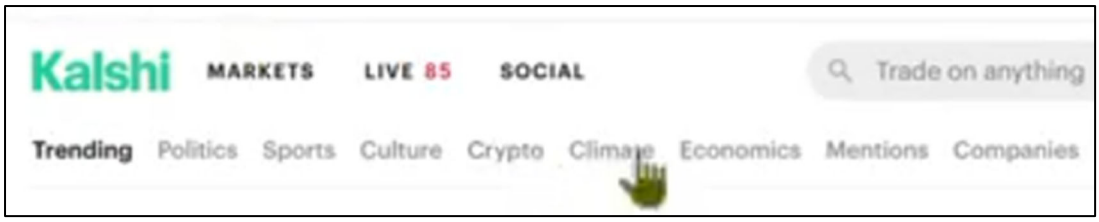
69. When a user enters their email address on the website, Google intercepts a "hashed" version of that email address, which Google is able to match to its existing profiles:

```
uap: Windows
uapv: 19.0.0
uaw: 0
ec_mode: a
em: tv.1~em.Kpoi2IsDEGTqhv8QTRyr9rFKhmwqSt8Tbe8TMLSf7Ls
ecsid: 1894465976.1772224703
```

[56] *Id.*

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

70. When a user makes a selection on the page, Google analytics intercepts the detailed URL showing the content of that selection.



en: page_view
gtm: 45be62p1v9238495171za20gzb9197087850zd9197087850xec
gcd: 13l3l3l3l1l1
dma: 0
tag_exp:
103116026~103200004~104527906~104528501~104573694~104684208~104684211~115616986~115938466~115938469~116024733
u_w: 3072
u_h: 1728
url: https%3A%2F%2Fkalshi.com%2Fcategory%2Fclimate
ref: https%3A%2F%2Fkalshi.com%2F
frm: 0
tiba: Climate%20Prediction%20Markets%20%26%20Weather%20Odds%20%7C%20Kalshi

71. Google also collects 3PIDs cookie values and other identifying cookie values as described above.

72. 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 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.

73. The information disclosed by Defendant allows Google to know the identities of specific individuals as well as their private information. This allows these companies, including Defendant, to profit from this information for targeted advertising purposes.

74. Through the above-listed Google tracking services, which Defendant used via the software code installed, integrated and embedded into the Website, Defendant disclosed its customers' legally protected information.

75. Defendant engages in this deceptive conduct for its own profit at the expense of its customers' privacy. Such disclosures are an invasion of privacy, lead to harassing targeted advertising, and violate federal and state law.

CLASS ALLEGATIONS

76. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Classes:

Nationwide Class: All natural persons in the United States who, during the class period, made a page selection or placed a wager on the Website.

California Subclass: All natural persons in the State of California who, during the class period, made a page selection or placed a wager on the Website.

77. Plaintiff reserves the right to modify the Class definitions, including by using subclasses, as appropriate based on further investigation and discovery obtained in the case.

78. The following people are excluded from the Classes: (1) any Judge presiding over this action and members of their family; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest (including current and former employees, officers, or directors); (3) persons who properly execute and file a timely request for exclusion from the Classes; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and

Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

79. **Numerosity:** The number of persons within the Classes is substantial and believed to amount to thousands of persons. It is, therefore, impractical to join each member of the Classes as a named plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Classes render joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Classes are ascertainable and identifiable from Defendant's and LinkedIn's records.

80. **Commonality and Predominance:** There are well-defined common questions of fact and law that exist as to all members of the Classes and that predominate over any questions affecting only individual members of the Classes. These common legal and factual questions, which do not vary between members of the Classes, and which may be determined without reference to the individual circumstances of any Class member, include, but are not limited to, the following: whether Defendant violated the ECPA, the CIPA §§ 631 and 632, and whether Plaintiff and the proposed Class members are entitled to damages, reasonable attorneys' fees, pre-judgment interest and costs of this suit.

81. **Typicality:** The claims of the named Plaintiff are typical of the claims of the Classes because the named Plaintiff, like all other class members, visited the Website and had his confidential electronic communications intercepted and disclosed to LinkedIn through LinkedIn's Insight Tag and Google through Google Analytics.

82. **Adequate Representation:** Plaintiff is an adequate representative of the Classes because his interests do not conflict with the interests of the Class members he seeks to represent, he has retained competent counsel experienced in prosecuting class actions, and he intends to prosecute this action vigorously. The interests of

members of the Classes will be fairly and adequately protected by Plaintiff and his counsel.

83. **Superiority:** The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of members of the Classes. Each individual member of the Classes may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSE OF ACTION

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

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

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

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

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

88. 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.

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

90. The transmission of PII and financial 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).

91. 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).

92. 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).

93. 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).

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

a. The computer codes and programs Defendant, LinkedIn, and Google 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, LinkedIn's, and Google's web and ad servers;

e. The plan the Defendant LinkedIn, and Google 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.

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

96. By utilizing and embedding the tracking technology provided by LinkedIn and Google 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).

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

98. Defendant intercepted communications that include, but are not necessarily limited to, communications to/from Plaintiff and Class Members regarding PII, including their identities and information related to the specific bets they placed. This confidential information is then monetized for targeted advertising purposes, among other things.

99. By intentionally disclosing or endeavoring to disclose Plaintiff's and Class Members' electronic communications to LinkedIn through the LinkedIn Insight Tag and to Google through Google Analytics, 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).

100. 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).

101. 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, the CIPA, and invasion of privacy, among others.

102. 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, Defendant violated numerous state privacy laws, including CIPA, and the common law for financial gain.

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

104. 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, all of whom are users of the Website, had a reasonable expectation that Defendant would not redirect their communications to LinkedIn without their knowledge or consent.

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

106. 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. § 2511, *et seq*. under 18 U.S.C. § 2520.

COUNT II
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 631(a)

107. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

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

109. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under CIPA § 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*
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> *Or*
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section

110. CIPA § 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); *see also Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, Section 631(a) applies to Internet communications.").

111. The LinkedIn Insight Tag and Google Analytics are each a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

112. LinkedIn and Google are each a "separate legal entity that offers [a] 'software-as-a-service' and not merely a passive device." *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Further, LinkedIn and Google each have the capability to use and does use the wiretapped information for their own purposes. Accordingly, LinkedIn and Google are each a third party to any communication between Plaintiff and California Subclass Members, on the one hand, and Defendant, on the other. *Id*. at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

113. At all relevant times, LinkedIn and Google willfully and without the consent of all parties to the communication, or in any unauthorized manner, read, attempted to read, and/or learned the contents or meaning of electronic communications of Plaintiff and members of the California Subclass, on the one hand, and Defendant, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

114. At all relevant times, LinkedIn and Google used or attempted to use the communications intercepted to, *inter alia*, monitor and improve their products and services.

115. At all relevant times, Defendant aided, agreed with, employed, permitted, or otherwise enabled LinkedIn and Google to wiretap Plaintiff and members of the

California Subclass through the LinkedIn Insight Tag and to accomplish the wrongful conduct at issue here.

116. Plaintiff and members of the California Subclass did not provide their prior consent LinkedIn's and Google's intentional access, interception, reading, learning, recording, collection, and usage of Plaintiff's and California Subclass members' electronic communications. Nor did Plaintiff and California Subclass members provide their prior consent to Defendant aiding, agreeing with, employing, permitting, or otherwise enabling LinkedIn's conduct.

117. The wiretapping of Plaintiff and California Subclass members occurred in California, where Plaintiff and California Subclass members accessed the Website and where the LinkedIn Insight Tag and Google Analytics—as enabled by Defendant—routed Plaintiff's and California Subclass members' electronic communications to their servers.

118. Pursuant to Cal. Penal Code § 637.2, Plaintiff and California Subclass members have been injured by Defendant's violations of CIPA § 631(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 631(a).

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

119. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

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

121. 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."

122. 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[.]"

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

124. 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 LinkedIn secretly eavesdrop upon or record this confidential information and their communications.

125. LinkedIn's and Google's tracking technology, i.e., the LinkedIn Insight Tag and Google Analytics, are all electronic amplifying or recording devices for purposes of § 632.

126. By contemporaneously intercepting and recording Plaintiff's and Class Members' confidential communications to Defendant through this technology, LinkedIn and Google eavesdropped and/or recorded confidential communications through an electronic amplifying or recording device in violation of § 632 of CIPA.

127. At no time did Plaintiff or Class Members consent to LinkedIn's and Google's conduct, nor could they reasonably expect that their communications would be overheard or recorded by LinkedIn.

128. LinkedIn and Google utilized Plaintiff's and Class Members' sensitive personal and financial information for its own purposes, including for targeted advertising.

129. Plaintiff and Class 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.

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

PRAYER FOR RELIEF

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

(a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order declaring that Defendant's conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) An award of statutory damages to the extent available;

(e) For punitive damages, as warranted, in an amount to be determined at trial;

(f) For prejudgment interest on all amounts awarded;

(g) For injunctive relief as pleaded or as the Court may deem proper; and

(h) For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Pursuant to Fed. R. Civ. P. 38(b)(1), Plaintiff demands a trial by jury of all issues so triable.

Dated: June 12, 2026

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Joshua R. Wilner*
Joshua R. Wilner

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

Attorney for Plaintiff