POTTER HANDY LLP
Mark D. Potter (SBN 166317)
James M. Treglio (SBN 228077)
Isabel Rose Masanque (SBN 292676)
Naomi Butler, Esq. (SBN 332664)
classactions@potterhandy.com
100 Pine St., Ste 1250
San Francisco, CA 94111
(415) 534-1911
Fax: (888) 422-5191

Attorneys for Plaintiff, on behalf of herself and all others similarly situated

SUPERIOR COURT OF CALIFORNIA

COUNTY OF ALAMEDA

THELMA KIMMONS, on behalf of herself and all others similarly situated

Plaintiffs,

v.

NFL ENTERPRISES LLC., a Delaware Limited Liability Company; and DOES 1-100, inclusive

Defendants.

CASE NO.

CLASS COMPLAINT FOR VIOLATIONS OF:

(1) PENAL CODE § 630 ET SEQ. (CALIFORNIA INVASION OF PRIVACY ACT);
(2) WIRETAP ACT, 28 U.S.C. § 2510 *et seq*.
(3) CALIFORNIA PENAL CODE § 502 (CALIFORNIA COMPUTER DATA ACCESS AND FRAUD ACT);
(4) ART. 1, § 1, CALIFORNIA CONSTITUTION (INVASION OF PRIVACY); and
(5) CAL. BUS. & PROF. CODE §17200, ET SEQ. (CALIFORNIA UNFAIR COMPETITION LAW)

DEMAND FOR JURY TRIAL

Class Representative Plaintiff Thelma Kimmons ("Plaintiff"), by and through her attorneys, individually and on behalf of others similarly situated, allege upon information and belief as follows:

NATURE OF THE ACTION

1. Defendant NFL Enterprises LLC., a Delaware Corporation ("Defendant") owns and operates a website https://www.nfl.com/ (the "Website" or "NFL").

2. When users visit the Website, Defendant causes numerous trackers and cookies developed and operated by Google, The Trade Desk, Rubicon Project, OpenX, LogRocket, Inc. and Shape Security (the "Trackers") to be installed on Website visitors' internet browsers. Defendant then uses these Trackers to collect Website visitors' identifying information, as well as dozens of other data points that reveal the users' behavior and activity on the Website, subjecting the user to unwanted and intrusive communications by would-be advertisers trying to sell the same or similar product to the user over and over and over again.

3. Because the Trackers intercept information about the Website visitors' interactions with the Website, the Trackers constitute unlawful wiretapping under Section 2511 of the Electronic Communications Privacy Act ("ECPA") and Section 631 of the California Invasion of Privacy Act ("CIPA").

4. Because the Trackers also capture Website visitors' "routing, addressing, or signaling information," the Trackers each constitute a "pen register" under Section 638.50(b) of CIPA. See *Greenley v. Kochava, Inc.*, 2023 WL 4833466 (S.D. Cal. July 27, 2023). By installing and using the Trackers without Plaintiff's prior consent and without a court order, Defendant violated CIPA section 638.51(a).

5. Plaintiff brings this action to prevent Defendant from further violating the privacy rights of California residents, and to recover statutory damages for Defendant's violation of the ECPA and CIPA.

PARTIES

6. Plaintiff Thelma Kimmons resides in San Leandro, California and has an intent to remain there, and is therefore a citizen of California. Plaintiff was in California when she visited the Website.

7. Defendant NFL Enterprises LLC., is a Delaware Limited Liability Company, with its principal place of business located in New York, New York.

VENUE AND JURISDICTION

8. This Court has jurisdiction over this action under California Code of Civil Procedure § 410.10. The aggregated amount of damages incurred by Plaintiff and the Class exceeds the $25,000 jurisdictional minimum of this Court. The amount in controversy as to the Plaintiff individually and each individual class member does not exceed $75,000, including interest and any pro rata award of attorneys' fees, costs, and damages. Venue is proper in this Court under California Code of Civil Procedure §§ 395(a) and 395.5 because Defendant does business in the State of California and in the County of Alameda. Defendant has obtained personal information about Plaintiff in the transaction of business in the County of Alameda which has caused both obligations and liability of Defendant to arise in the County of Alameda.

I. INTRODUCTION

A. The California Invasion of Privacy Act

9. The California Legislature enacted CIPA to protect certain privacy rights of California citizens. The California 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.

10. Although CIPA was enacted before the dawn of the Internet, "the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc.*, 2013 WL 5423918, at *21 (N.D. Cal. Sept. 26, 2013); see also *Greenley, supra*, 2023 WL 4833466, at *15 (referencing CIPA's "expansive language" when finding software was a "pen register"); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, [CIPA]

Section 631(a) applies to Internet communications."). This accords with the fact that, "when faced with two possible interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection." *Matera v. Google Inc.*, 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

11. Individuals may bring an action against the violator of any provision of CIPA—including CIPA sections 630 and 638.51—for $5,000 per violation. Cal. Penal Code § 637.2(a)(1).

B. The Federal Wiretap Act

12. The ECPA was originally enacted in October 1986 to extend privacy protections to emerging technologies. In drafting the legislation, Congress acknowledged that "[t]he dramatic development of the Internet has transformed methods of gathering, processing and sharing information." Senate Judiciary Committee Report (S. Rep. No. 99-541, 1986). Therefore, the statute aimed to address "individuals' concerns that a sufficient degree of privacy and the integrity of personal information are maintained in an age of modern communications and information storage." *Id.*

13. Although limiting overreach by law enforcement was one of the main purposes of the statute, the ECPA explicitly applies to private actors, including "any individual, partnership, association, joint stock company, trust, or corporation" who illegally intercepts, or attempts to intercept, "the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. 18 U.S.C.A. § 2510(4)(6).

14. The statute authorizes individuals to recover civil damages of up to $10,000 from any person who violates the provisions of the ECPA.

II. DEFENDANT ILLEGALLY INTERCEPTS THE CONTENTS OF ELECTRONIC AND WIRE COMMUNICATIONS AND ILLEGALLY CAPTURES IDENTIFYING INFORMATION

A. Overview of Website Tracking Technology

15. Website tracking technology originally consisted of simple tools such as first-party cookies accessible only by the domain (website address) that set the cookies. However, as online

advertising and analytics advanced, the industry increasingly relied on third party cookies which are set and accessed by domains other than the website a user originally visited. Over time, websites began implementing techniques which enabled the sharing of data collected by first-party cookies with third party domains, giving them access to user activity.

16. In addition to first-party and third-party cookies, the technology has further evolved into an advanced and interconnected system of methods that are capable of tracking the behavior of users across multiple websites, devices, and sessions using tools such as pixels, device "fingerprinting," and other real-time data exchanges.

i. Cookies

17. A cookie is a small text string with data created by a website's server and transmitted to a web browser, which then stores the string on the user's device. When the user revisits the website, the browser sends the string along with the HTTP request, allowing the tracker to recognize the user and build sophisticated profiles. These cookies can remain on the device for years, enabling long-term tracking and profiling.

18. When the same third-party tracker appears on multiple websites, it can use its cookies to build a comprehensive profile of users by merging data from various sources. This allows for detailed tracking of individuals' browsing habits, preferences, and behaviors across the internet.

19. Trackers and their associated cookies are installed and operate automatically and invisibly when users visit websites. Users are generally unaware that their data is being collected and shared with third parties or that cookies are storing information on their device, as the process occurs in the background without any visible signs.

ii. Pixels

20. Pixel "events" are JavaScript tracking codes that send detailed information about user actions to third-party servers, such as Facebook and Google, in real-time.

21. Common user events tracked by Pixels include page views (when a user loads a specific webpage), content views (when a user interacts with a specific piece of content on a webpage), clicks (when a user selects a specific element on a webpage), form submissions (text or

data a user inputs into a field on a webpage), and search queries (terms or phrases a user enters into a search box on a webpage).

22. Importantly, Pixel events represent a coordinated surveillance arrangement between websites and tech giants, like Facebook. A website lets Facebook watch their customers, and Facebook provides free tracking and analytics in exchange for data. Both profit from the arrangement at the expense of consumer privacy.

iii. Device fingerprinting

23. Device fingerprinting refers to a broad category of techniques that are used to identify a user's device across visits (also called "sessions"). It works by collecting information about a user's hardware and software attributes, such as browser type, operating system, screen resolution, installed fonts, and time zone and language settings. The combination of these attributes becomes the user's "device fingerprint."

24. When combined, the probability that two users have identical attributes and settings is very low, even if they have the same type of device or browser. This is because the technical characteristics still vary based on individual configuration and software versions, which allow trackers to accurately and uniquely identify users without relying on cookies.

25. Canvas fingerprinting is a specific type of device fingerprinting that identifies and tracks a user's device based on these unique characteristics. It works by downloading a Javascript code when a user visits a webpage and runs it in the user's browser. This initiates a process completely invisible to a user.

26. The Javascript creates an invisible HTML canvas element—like a digital drawing board—and draws texts, shapes, and emojis on the canvas using various fonts and colors. The script then reads back the exact pixel values of what it just drew and runs these pixels through a mathematical function (a "hash") that converts them into a "unique identifier." This unique identifier becomes the user's "device fingerprint."

27. The Javascript sends this fingerprint to a server, and the server uses it to recognize a user on future visits, without the use of any cookies.

28. The reason this process creates a unique identifier is because devices render graphics slightly differently based on their graphics card model, driver version, installed fonts, operating systems, screen resolution, and color calibration. These tiny variations create a unique pattern—like a fingerprint—that is remarkably stable and hard to change. This fingerprint persists even if a user clears their browser data.

iv. IP Addresses

29. IP addresses serve an important functional role on the internet by acting like a digital postal address that allows devices to send and receive data.

30. An IP address is a unique identifier for a device, which is expressed as four sets of numbers separated by periods (e.g., 192.168.123.132). The first two sets of numbers indicate what network the device is on (e.g., 192.168), and the second two sets of numbers identify the specific device (e.g., 123.132).

31. Functionally, to make a website load on a user's internet browser, the browser sends an "HTTP request" to Defendant's server where the relevant website data is stored.

32. In response to the request, Defendant's server sends an HTTP response back to the browser with a set of instructions.

33. The server's instructions include how to properly display the Website—e.g., what images to load, what text should appear, or what music should play.

34. Thus, the IP address enables a device to communicate with another device, such as a computer's browser communicating with a server.

35. However, IP addresses can also be used as potential user identifiers, especially when used in combination with additional data collected from the techniques described above.

36. Through an IP address, the specific device's state, city, and zip code can be determined.

37. Much like a telephone number, an IP address is a unique numerical code associated with a specific internet-connected device or household Thus, knowing a user's IP address—and therefore geographical location—"provide[s] a level of specificity previously unfound in marketing."

38. An IP address allows advertisers to (i) "[t]arget [customers by] countries, cities, neighborhoods, and … postal code" and (ii) "to target specific households, businesses[,] and even individuals with ads that are relevant to their interests." Indeed, "IP targeting is one of the most targeted marketing techniques [companies] can employ to spread the word about [a] product or service" because "[c]ompanies can use an IP address … to personally identify individuals."

39. For example, businesses who are trying to reach college-aged demographics can target devices on college campuses by sending advertisements to IP addresses associated with college-wide Wi-Fis. Or, for a job fair in specific city, companies can send advertisements to only those in the general location of the upcoming event. In addition to "reach[ing] their target audience with greater precision," businesses are incentivized to use a customer's IP address because it "can be more cost-effective than other forms of advertising." "By targeting specific households or businesses, businesses can avoid wasting money on ads that are unlikely to be seen by their target audience."

40. In addition, "IP address targeting can help businesses to improve their overall marketing strategy." "By analyzing data on which households or businesses are responding to their ads, businesses can refine their targeting strategy and improve their overall marketing efforts."

41. Public IP addresses enable companies to monitor user interactions and behaviors across various websites and construct comprehensive profiles of users' browsing habits and preferences tied to their location.

42. They are especially effective in identifying and tracking specific individuals. As individuals use their devices across different locations (e.g., home, work, coffee shops, or other places), each location is assigned a distinct public IP address.

43. By tracking these patterns of movement between different IP addresses, businesses are able to build detailed profiles of individual users' daily routines and behaviors, which allows them to differentiate an individual from others who might be accessing the internet using the same public IP address (e.g., other members of the same household).

44. For instance, if an individual visits websites on their laptop using their home IP address in the morning, their work IP address during the day, and returns to their home IP address in the evening, this sequence forms a distinctive pattern that can be used to identify that individual.

45. For these reasons, Europe's General Data Protection Regulation classifies IP addresses as "personal data," since they can potentially be employed "to identify an individual."

v. Session recording

46. Session recording tools capture a comprehensive, time-stamped log of every user interaction on a website, together with synchronized snapshots of the webpage's underlying structure (the Document Object Model, or DOM). The vendor's servers store this event log and DOM data as structured records and can later replay the session in a browser-based player that visually reconstructs what the user saw and did. They monitor mouse movements (every pixel traveled), clicks (what you clicked and where), scrolling (how far, how fast), form inputs (what you type, including deletions), page navigation (every page visited), and time spent on each element.

47. Importantly, session recording is qualitatively different from cookies or conventional analytics. Where cookies identify visitors and analytics aggregate pageview counts, session recording produces an event-by-event behavioral log—a structured, queryable record of every discrete action the user takes on the page. This log can be filtered and searched (for example, to retrieve every visitor who typed specific text into a form field, or who hovered over a specific button for more than a given duration), and it can be replayed visually as a reconstruction of the user's session. This is a qualitatively more invasive form of surveillance than cookies or pageview analytics.

48. Session recorders are highly invasive because of the level of nuance captured during a session. Because it captures deleted content, if a user types a message and deletes it, the recording captures exactly what they explicitly chose not to submit. It also reveals other user behaviors such as user hesitation, since it can record how long a use hovered over a "Buy Now" button before clicking on it (or not).

49. Session recorders have the potential to capture sensitive data such as passwords, credit cards, and health information, if not properly configured.

50. Moreover, real people at the companies who own the session recording technology have the ability to watch replays of user sessions and recordings are stored indefinitely for analysis.

B. Tracking Technology on Defendant's Website

51. Using a combination of the tracking technologies described above, Defendant actively shared user data with multiple third parties, including Google, The Trade Desk, Rubicon Project, OpenX, LogRocket, Inc. and Shape Security by deploying tools and scripts developed by these companies that collected, transmitted, and processed information from users who accessed the Website.

52. Specifically, forensic testing confirmed that the Website deployed 182 third-party trackers, including 24 cookies, 4 different canvas fingerprints, and 1 session recorder. Defendant further shared data collected by these trackers with four major advertising networks.

i. Session Recorders

53. Defendant deployed a session recorder on the Website using scripts and tools developed and operated by LogRocket, Inc. that intercepted, recorded, and transmitted Plaintiff's and Class Members' interactions with Defendant's in real time.

54. The session replay technology captures the full Document Object Model ("DOM") state and a reconstructed visual replay of each user's browsing session, enabling the third-party provider to reproduce exactly what the user saw, viewed, selected, and interacted with during the visit.

55. The session replay technology further captured information entered into the Website into input fields, including information typed search bars and other interactive form fields. The session replay technology also recorded users' keystrokes entered into website inpute fields, including the sequence and timing of individual keystrokes.

56. In addition, the session replay technology continuously tracked and recorded users' mouse movements, cursor locations, clicks, click coordinates, hover events, and navigation paths throughout each browsing session. The information enabled the creation of detailed behavioral profiles reflecting how users navigated and interacted with Defendant's website.

57. The session replay technology further recorded users' scrolling behavior, including scroll depth scrolling speed, scrolling direction, and the portions of webpages viewed by users. This information revealed users' engagement with webpage content and their reading and browsing behavior.

ii. Google Tracking Technology

58. Google is one of the largest advertising companies in the country. To date, Google generates nearly 77.8% of its revenue through advertising bringing in a grand total of $305.6 billion. Google's advertising business has been extremely successful due, in large part, to Google's ability to target people at a granular level.

59. Defendant embedded Google Ads and Google DoubleClick scripts on its Website, which allowed it to actively share detailed information about users with Google, including device and browser characteristics, page views, and content views.

60. The Google Ads and Google DoubleClick scripts collect and transmit information about users' behavior across multiple websites, enabling Google to build detailed behavioral profiles for each user. These profiles are shared with advertisers within the Google Ad Manager ecosystem, allowing Google to show users particular advertisements based on their activity—a practice commonly known as "audience targeting."

61. Additionally, the Website uses Google Tag Manager to deploy a script to perform canvas fingerprinting. This unique identifier is what allows Defendant and Google to track users across multiple websites.

62. Finally, if the user is logged into their Google account when visiting the Website, Google receives third party cookies allowing it to link the data collected by the code to the specific Google user, and derive demographic information about that user, such as age and gender.

iii. Advertising Networks

63. An advertising network is a system that connects advertisers with websites by collecting data about how users interact with a website and delivering relevant ads based on the user's behavior. These advertising networks use unique identifiers—such as cookies or device

fingerprints—to persistently monitor users across different websites and build a highly detailed behavioral profile of each user over time.

64. Defendant embedded the code for four different advertising networks on its Website, including Google, The Trade Desk, Rubicon Project, OpenX, LogRocket, Inc. and Shape Security as well as the Google and Meta ad networks described above. By embedding this code, the Website automatically transmitted extensive information about users' browsing behavior and identity to each of these third-party networks, including page views, product views, content interaction, IP addresses, and device and browser characteristics.

65. These advertising networks also collect data on parameters that indicate how likely a user may buy a product or service—commonly known as "purchase intent signals." The advertising networks then uses this data to show users ads based on their browsing behavior on Defendant's Website and other websites.

v. Canvas Fingerprinting

66. Defendant implements extensive canvas fingerprinting on the Website across multiple third-party services, deploying 4 separate scripts from Google Tag Manager and Shape Security.

67. By integrating 4 separate fingerprinting instances across multiple vendors, this creates a highly unique and persistent identifier that can track users across sessions and websites.

68. All four instances capture the full trifecta of canvas-based fingerprinting signals: font rendering (how the browser renders specific typefaces at the pixel level), geometry rendering (how the browser draws shapes, curves, and paths), and data URL extraction (reading back the raw pixel data from the canvas as a base64-encoded image). Together, these produce a highly detailed, device-specific graphical signature reflecting the user's GPU, graphics drivers, operating system font library, and browser rendering engine.

69. Three Google Tag Manager instances are tied to Google Ads (AW-810518499) and Campaign Manager (DC-13319313), which are advertising and conversion tracking platforms. These instances are unambiguously collecting canvas fingerprints for cross-site advertising attribution and user tracking purposes, raising significantly stronger privacy concerns.

70. The information on consumer behavior gathered by has tremendous value to advertisers and to the Defendant. Similar market research on consumer behavior can increase overall sales by millions of dollars. In this way, Defendant and the advertisers have stolen information from Plaintiff, and the Class Members, of significant value. Participants in focus groups, for instance, are regularly paid $30-$500 per session. But instead of paying Plaintiff and the Class, Defendant and the Third Parties stole the information from Plaintiff and the Class.

C. Defendant Aided and Abetted Third-Party Interception by Installing and Using Trackers on the Website to Collect Plaintiff's and Class Member's Communications Without Consent or Court Order

71. Section 631 of CIPA prohibits the interception of communications without the consent of all parties and provides that a person who aids, abets, employs, or conspires with another to intercept communications may also be liable. Cal. Penal Code § 631(a).

72. In the internet context, courts repeatedly recognize that a third party becomes an unauthorized interceptor when a website embeds tracking technology that captures user communications in real time and permits the third party to use the intercepted communications for its owner commercial purposes. See *Smith v. Rack Room Shoes, Inc*., 2025 WL 1085169 at *4 (N.D. Cal. Apr. 4, 2025)(rejecting the argument that the trackers were not unauthorized third parties but "extensions" of the website); *Ambriz v. Google, LLC*, 2025 WL 830450 (third party trackers who have the capability to use the information transmitted are unauthorized parties regardless of their intent).

73. Defendant owns and operates the Website, https://www.nfl.com/, which provides information relating to professional football, including news, schedules, scores, standings, statistics, videos, and other content concerning the National Football League and its teams, players, and events.

74. Defendant has long incorporated the code of the Trackers into the code of its Website, including when Plaintiff and other users visited the Website. Thus, when Plaintiff and other users visited the Website, the Website caused the Trackers to be installed on Plaintiff's and other users' browsers.

75. As outlined above, when a user visits the Website, the Website's code—as programmed by Defendant—installs the Trackers onto the user's browser so that it can be executed within the context of that website. Scripts, including tracking software, must be (re-)installed into the browser for each website that uses them, and so Defendant is solely responsible for the installation of the tracking software that will execute on its website.

76. Upon installing the Trackers on its Website, Defendant uses the Trackers to collect the identifying information and user behavior and activity from Class Members and transmits that data to the third-parties that developed and operate the Trackers in real time.

77. The operators of the Trackers then use the correlated information of users, including those of Plaintiff and Class Members, for their own commercial purposes, including targeted advertising, marketing, and website analytics.

78. At no time prior to the installation and use of the Trackers on Plaintiff's and Class Members' browsers, or prior to the use of the Trackers, did Defendant procure Plaintiff's and Class Members' consent for such conduct. Nor did Defendant obtain a court order to install or use the Trackers or to transmit the information collected to the unauthorized third-party Trackers.

79. Notably, while there is a pop-up banner which allows website visitors to opt-out cookies, this banner gives users a false and misleading sense of security over their online privacy for two important reasons.

80. First, Defendant programmed the Trackers to deploy immediately upon a user landing on the Website. Before a user can configure their privacy choices, the Trackers have already begun fingerprinting the user's device, recording the user's session, and downloading cookies and pixels onto their browser.

81. Second, even if a user chooses to opt-out of the cookies, it does not have any effect on session recorders, canvas fingerprinting, or other scripts which do not rely on cookies to operate. Notably, even when a user chooses to opt-out of the cookies, the Website continues to run 186 third party trackers, including 25 cookies, 4 canvas fingerprints, and 1 session recorder.

82. Therefore, Defendant failed to obtain consent from Plaintiff and the Class Members prior to installing and using the Trackers on the Website, in violation of CIPA Sections 631 and 638.51.

83. Under the ECPA, the consent of one party is also insufficient where "such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. § 2511(2)(d); see also, *Doe v. Meta Platforms, Inc.* (N.D. Cal. 2023) 690 F. Supp. 3d 1064, 1077.

84. Because Defendant's interception and disclosure of the communications also violates CIPA, as well as California's Comprehensive Data Access and Fraud Act and the right to privacy under the California Constitution, as well as constituting a fraudulent and unlawful business practice under the Unfair Competition Law, discussed *infra*, consent by United alone is insufficient to shield it from liability under the ECPA. See *Smith v. Rack Room Shoes, Inc*., *supra,* 2025 WL 1085169 at *5 (the website tracking allegations are analogous to the purpose of engaging in a HIPPA violation, which courts consistently find constitutes an independent prohibited purpose.").

D. Defendant's Conduct Constitutes an Unauthorized Interception of the Contents of Communications under CIPA and the ECPA

85. Because the Trackers intercept information about the Website visitors' interactions with the Website, Defendant's use of the Trackers constitutes an unlawful interception and disclosure of an "electronic communication" under Section 2511 of the ECPA.

86. Defendant's use of the Trackers also constitutes an "unauthorized connection" which "reads, or attempts to read, or to learn the contents or meaning of [a] message, report, or communication" under Section 631 of CIPA.

87. "Contents" of a communication refer to "any information concerning the substance, purport, or meaning of a communication." *In re Zynga Priv. Litig*. (9th Cir. 2014)750 F.3d 1098, 1106–07)(internal quotations omitted). This includes button clicks, viewing history, cart history, or any other information that reveals a user's personal interests, queries, or habits. See also, *Mikulsky v. Bloomingdale's, LLC*, 2025 WL 1718225, at *1 (9th Cir. June 20, 2025)(session recording technology constitutes "contents" for the purposes of Section 631 of CIPA).

88. The communications intercepted by the Trackers, which include a session recorder are "contents" within the meaning of CIPA and the ECPA because they reveal substantive information about the user's interests, preferences, and potential consumer behavior.

E. Defendant's Conduct Constitutes an Illegal Pen Register and Trap and Trace Device Under CIPA

89. CIPA section 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

90. A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

91. A "trap and trace device" is a "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(b).

92. In plain English, a "pen register" is a "device or process" that records outgoing information, while a "trap and trace device" is a "device or process" that records incoming information.

93. Historically, law enforcement used "pen registers" to record the numbers of outgoing calls from a particular telephone line, while law enforcement used "trap and trace devices" to record the numbers of incoming calls to that particular telephone line. As technology advanced, however, courts have expanded the application of these surveillance devices.

94. For example, if a user sends an email, a "pen register" might record the email address it was sent from, the email address(es) the email was sent to, and the subject line—because this is the user's outgoing information. On the other hand, if that same user receives an email, a "trap and trace device" might record the email address it was sent from, the email address it was sent to, and the subject line—because this is incoming information that is being sent to that same user.

95. Defendant executes each of the Trackers on the user's browser for marketing and analytics purposes, and the Trackers collect information that identifies the outgoing "routing, addressing, or signaling information" of the user by through the collection of IP addresses through the 182 third-party trackers loaded in the pre-consent state (and 186 trackers loaded after the user affirmatively opted out of non-essential cookies), as described above, as well as the device fingerprinting techniques and unique identifiers described above. Accordingly, the Trackers are each "pen registers."

96. The Trackers are "process" because it is "software that identifies consumers, gathers data, and correlates that data." *Greenley, supra*, 2023 WL 4833466, at *15.

97. The Trackers are a "device" because "in order for software to work it must be ran on some kind of computing device." *James v. Walt Disney Co*., 701 F.Supp.3d 942 (N.D. Cal. Nov. 8, 2023).

98. Because the Trackers capture outgoing information that capture the source of a communication, they are a "pen register" for the purposes of CIPA section 638.50(b).

F. Defendant's Conduct Constitutes An Invasion Of Plaintiff's And Class Members' Privacy

99. The collection of Plaintiff's and Class Members' personally identifying, nonanonymized identifying information, and Website activity through Defendant's installation and use of the Trackers constitutes an invasion of privacy.

100. As alleged herein, the Trackers are designed to analyze Website data and marketing campaigns, conduct targeted advertising, and boost Defendant's revenue, all through their surreptitious collection of Plaintiff's and Class Members' data.

III. PLAINTIFF'S AND THE CLASS MEMBERS' EXPERIENCES

101. Plaintiff Thelma Kimmons visited the Website in and around January 2026 to view live scores and track game schedules as a fan of the San Francisco 49ers.

102. Each of the Trackers described above are found on the Website. Therefore, when Plaintiff visited the Website, the Website's code—as programmed by Defendant—caused the Trackers to be installed on Plaintiff's browsers.

103. Defendant shared Plaintiff's data with each of the third-party canvas fingerprinting operators, including Google Tag Manager and Shape Security to create a highly unique identifier for the Plaintiff.

104. The Trackers used the canvas fingerprints to track Plaintiff's activity not only on the Website during his/her initial visit, but also across other websites and during subsequent visits.

105. Additionally, the session recorder on the Website immediately began recording Plaintiff's entire browsing session. The Website captured Plaintiff's every mouse movement and click as she searched and browsed the Website. Additionally, the session recorder on the Website captured the keystrokes Plaintiff entered into the search field, regardless of whether she deleted or submitted the entry.

106. Defendant used the information collected by the Trackers and shared it with third parties to analyze Website data and marketing campaigns, conduct targeted advertising based on Plaintiff's locations, and ultimately boost Defendant's and advertisers' revenue.

107. Although Defendant uses at least several different Trackers on the Website, they all operate in the same manner and perform the same function, i.e., collecting Plaintiff's and Class Members' identifying information and Website activity. Thus, at any given time a user visits the Website, Defendant will cause one of the Trackers to be installed on users' browsers for the purpose of collecting IP addresses and other user behavior data associated with the Plaintiff and Class Members.

108. Plaintiff and Class Members did not provide their prior consent to Defendant to install or use the Trackers on their browsers.

109. Defendant did not obtain a court order before installing or using the Trackers.

110. Thus, like Plaintiffs, Class Members have also had their privacy invaded by Defendant's violations of CIPA sections 631 and 638.51(a).

111. Plaintiff seeks to access the Website without third-party tracking technologies intercepting and disclosing her communications or personal data, or, alternatively, to be provided with a meaningful choice regarding what data is collected.

CLASS ACTION ALLEGATIONS

112. Class Representative Plaintiff brings this action on their own behalf and on behalf of all other persons similarly situated. The putative class that Class Representative Plaintiffs seek to represent is composed of:

Nationwide Class

All United States residents who accessed the Website and had their identifying information and website behavior data collected by the Trackers without consent and/or despite declining consent two years prior to the filing date of this Complaint through the date of an order granting class certification and/or a motion for preliminary approval of class action settlement (hereinafter the "Class").

California subclass

All California residents who accessed the Website in California and had their identifying information and website behavior data collected by the Trackers without consent and/or despite declining consent one year prior to the filing date of this Complaint through the date of an order granting class certification and/or a motion for preliminary approval of class action settlement (hereinafter the "Subclass").

113. Excluded from the Class are the natural persons who are directors, and officers, of the Defendant, as well as judicial officers and attorneys of record, their families, and their staff who are assigned to this action. Class Representative Plaintiff expressly disclaims that they are seeking a class-wide recovery for personal injuries attributable to Defendant's conduct.

114. Plaintiff is informed and believe that the members of the Class are so numerous that joinder of all members is impracticable. While the exact number of the Class members is unknown to Class Representative Plaintiff at this time, such information can be ascertained through appropriate discovery, from records maintained by Defendant.

115. There is a well-defined community of interest among the members of the Class because common questions of law and fact predominate, Class Representative Plaintiff's claims are typical of the members of the class, and Class Representative Plaintiff can fairly and adequately represent the interests of the Class.

116. Common questions of law and fact exist as to all members of the Class and

predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class are:

(a) Whether the Defendant unlawfully read and/or intercepted communications by Plaintiff and members of the Class through use of the Trackers;

(b) Whether the Defendant unlawfully collected routing, addressing, and signaling information from Plaintiff and members of the Class through use of the Trackers;

(c) Whether Defendant violated CIPA section 631(a);

(d) Whether Defendant violated CIPA section 638.51(a);

(e) Whether Defendant violated the Wiretap Act, 28 U.S.C. section 2510 et seq.;

(f) Whether the Trackers are "pen registers" pursuant to Cal. Penal Code section 638.50(b);

(g) Whether Defendant sought or obtained prior consent—express or otherwise—from Plaintiff and the Class;

(h) Whether Defendant benefitted financially from the information taken by the Trackers, and the value of the information taken;

(i) Whether the theft of this information constitutes a violation of the California Unfair Competition Law;

(j) Whether Defendant sought or obtained a court order for its use of the Trackers; and

(k) Whether Plaintiff and members of the Class are entitled to actual damages, statutory damages, or restitutionary disgorgement for the aforementioned violations.

Class Representative Plaintiff's claims are typical of those of the other Class members because Class Representative Plaintiffs, like every other Class member, were exposed to virtually identical conduct and are entitled to the same relief under the CIPA.

117. Class Representative Plaintiff will fairly and adequately protect the interests of the Class. Moreover, Class Representative Plaintiff has no interest that is contrary to or in conflict with those of the Class they seek to represent during the Class Period. In addition, Class Representative Plaintiff has retained competent counsel experienced in class action litigation to further ensure such protection and intend to prosecute this action vigorously.

118. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which would establish incompatible standards of conduct for the Defendant in the State of California and would lead to repetitious trials of the numerous common questions of fact and law in the State of California. Class Representative Plaintiff knows of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action. As a result, a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

119. Proper and sufficient notice of this action may be provided to the Class members through direct mail.

120. Moreover, the Class members' individual damages are insufficient to justify the cost of litigation, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Absent certification of this action as a class action, Class Representative Plaintiff and the members of the Class will continue to be damaged by the practices of Defendant.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the California Invasion of Privacy Act,

Cal. Penal Code § 630, et seq.(a)

(California subclass only)

121. The allegations of the preceding paragraphs are incorporated by reference as if fully set forth herein.

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

123. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638.

124. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq*. ("CIPA") finding that "advances in science and technology have led to

the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id*. § 630. Thus, the intent behind CIPA is "to protect the right of privacy of the people of this state." *Id*.

125. Cal. Pen. Code § 631(a) imposes liability upon: "Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section . . . ."

126. Defendant used tracking software on the Website to intercept and collect information about Website visitors' behavior and activity on the Website.

127. CIPA section 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

128. A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

129. The Trackers are "pen registers" because they are "device[s] or process[es]" that "capture[d]" the "routing, addressing, or signaling information"—the IP address—from the electronic communications transmitted by Plaintiff's and the Class's computers or smartphones. Cal. Penal Code § 638.50(b).

130. At all relevant times, Defendant installed the Trackers—which are pen registers—on Plaintiff's and Class Members' browsers and used the Trackers to collect identifying

information of Plaintiff and Class Members, including IP addresses.

131. Plaintiff and Class Members did not provide their prior consent to Defendant's installation or use of the Trackers.

132. Defendant did not obtain a court order to install or use the Trackers.

133. Pursuant to Cal. Penal Code section 637.2, Plaintiff and Class Members have been injured by Defendant's violations of CIPA section 631(a) and 638.51(a), and each seeks injunction and statutory damages of $5,000 for each of Defendant's violations of CIPA section 631(a) and 638.51(a).

SECOND CAUSE OF ACTION

Violation of the Wiretap Act

Title 1 of the Electronic Communications Privacy Act ("ECPA") (18 U.S.C. § 2510, *et seq*.)

134. The allegations of the preceding paragraphs are incorporated by reference as if fully set forth herein.

135. The Wiretap Act prohibits the intentional interception, use, and/or disclosure of the contents of any wire, oral, or electronic communication. 18 U.S.C. § 2511(a), (c), (d).

136. "Intercept" is defined as "the aural or other 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).

137. "Contents" is defined as "includ[ing] any information concerning the substance, purport, or meaning of that communication[.]" 18 U.S.C. § 2510(8).

138. "Person" is defined as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation[.]" 18 U.S.C. § 2510(6).

139. Plaintiff is an individual and is therefore a "person" for purposes of § 2510(6).

140. Defendant is a corporation and is therefore a "person" for purposes of § 2510(6).

141. When Plaintiff and Class Members accessed Defendant's website, Defendant violated 18 U.S.C. § 2511(1)(a) when it installed Trackers on Plaintiff's browsers, which then

intercepted and collected Plaintiff's identifying information, as well as dozens of other data points that revealed Plaintiff's and Class Members' behavior and activity on the Website without their consent.

142. When Plaintiff and Class Members accessed Defendant's website, Defendant violated 18 U.S.C. § 2511(1)(c) when it disclosed Plaintiff's and Class Members' identifying information, behavior, and activity, obtained from the Trackers to third parties without their consent.

143. When Plaintiff and Class Members accessed Defendant's website, Defendant violated 18 U.S.C. § 2511(1)(d) when it used Plaintiff's identifying information, behavior, and activity obtained from the Trackers for its own advertising and marketing purposes without their consent.

144. As a result of Defendant's violations of the Wiretap Act, Plaintiff and Class Members have suffered harm and injury, including but not limited to the invasion of their privacy rights, loss of their information and loss of money and costs incurred, all of which have ascertainable value to be proven at trial.

145. Pursuant to 18 U.S.C. § 2520, Plaintiff has been damaged by the interception, disclosure, and/or use of their communications in violation of the ECPA and are each entitled to: (1) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiff and any profits made by Defendants as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; and (2) reasonable attorneys' fees and other litigation costs reasonably incurred.

THIRD CAUSE OF ACTION

Violation of the California Computer Data Access and Fraud Act

(California Penal Code § 502)

(California subclass only)

146. The allegations of the preceding paragraphs are incorporated by reference as if fully set forth herein.

147. The California Legislature enacted the CDAFA with the intent to "expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering,

interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a).

148. The Legislature further declared that "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data." Cal. Penal Code § 502(a).

149. For purposes of the statute, a number of definitions were provided. The term "access" means to "gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network." Cal. Penal Code § 502(b)(1).

150. The term "computer program or software" is defined as "a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions." Cal. Penal Code § 502(b)(3).

151. The term "computer system" refers to "a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions, including but not limited to, logic, arithmetic, data storage and retrieval, communication, and control." Cal. Penal Code § 502(b)(5).

152. Plaintiff's and Class members' web browsers used to access the Website are "computer software," and the computers on which Plaintiff and Class members used their web browsers constitute computers or "computer systems" within the scope of the CDAFA.

153. The statute also defines the term "data" to mean a "representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions." The statute further provides that data may be in "any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device." Cal. Penal Code § 502(b)(8).

154. As discussed above, a website cookie, including a third-party tracker cookie, and an

IP address are both "data" within the meaning of the statute.

155. Under California Penal Code § 502(c)(1), it is unlawful to knowingly access and without permission alter, damage, delete, destroy, or otherwise use any data, computer, computer system, or computer network in order to…wrongfully control or obtain money, property or data. Cal. Penal Code § 502(c)(1).

156. The statute also makes it unlawful to knowingly access and without permission take, copy, or make use of any data from a computer, computer system, or computer network. Cal. Penal Code § 502(c)(2).

157. The CDAFA further prohibits any person from knowingly accessing and without permission adding, altering, damaging, or destroying any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network. Cal. Penal Code § 502(c)(4).

158. Under subsections (6) and (7) of Penal Code § 502(c), a person also may not knowingly and without permission (i) provide or assist in providing a means of accessing or (ii) access or cause to be accessed any computer, computer system, or computer network. Cal. Penal Code §§ 502(c)(6) and (7).

159. Based on Defendant's unauthorized installation and storage of third-party tracking technology on Plaintiff's and Class members' web browsers, as alleged above, Defendant knowingly accessed and without permission altered and used Plaintiff's and Class members' data and computer systems in violation of Penal Code § 502(c)(1).

160. Similarly, the installation of the Trackers violates subsection (c)(4) because Defendant added and altered data and computer software on Plaintiff's and Class members' computers or computer systems. Cal. Penal Code § 502(c)(4).

161. By installing third-party tracking technology, Defendant also knowingly and without permission provided those trackers a means of accessing and/or caused to be accessed Plaintiff's and Class members' computers, computer systems, and/or computer networks in violation of Penal Code §§ 502(c)(6) and (7).

162. Further, Defendant's unauthorized collection and disclosure of Plaintiff's and Class

members' personally identifying and addressing information to undisclosed third parties violates Penal Code § 502(c)(2) because Defendant took and made use of data, including IP addresses, from Plaintiff's and Class members' computers, computer systems, or computer networks.

163. Plaintiff and Class members are citizens of California, and used their computers, computer systems, and/or computer networks in California. Defendant accessed or caused to be accessed Plaintiff's and Class members' data and other personally identifying information from within California.

164. Defendant was unjustly enriched by accessing, acquiring, taking, and using Plaintiff's and Class members' data and computer systems without their permission or consent, and using all of that identifying information to maximize revenue from selling advertising space on the Website and for Defendant's own financial benefit. Defendant has been unjustly enriched in an amount to be determined at trial.

165. As a direct and proximate result of Defendant's violations of the CDAFA, Plaintiff and Class members have suffered damages. Under Penal Code § 502(e)(1), Plaintiff and Class members are entitled to compensatory damages, injunctive relief, and other equitable relief in an amount to be determined at trial.

166. Plaintiff and Class members also are entitled to an award of reasonable attorneys' fees and costs under Penal Code § 502(e)(2).

FOURTH CAUSE OF ACTION

Invasion of Privacy

(Violation of Art. 1, § 1, California Constitution)

(California subclass only)

167. The allegations of the preceding paragraphs are incorporated by reference as if fully set forth herein.

168. "Privacy" is listed in Article I, Section 1, of the California Constitution as a fundamental right of all Californians. That section of the Constitution provides as follows: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and

obtaining safety, happiness, and privacy." Cal. Const. art. I, § 1.

169. The right to privacy in California's Constitution creates a right of action against private entities such as Defendant. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of social norms.

170. Plaintiff and Class members have a legally protected privacy interest in their personally identifying information and addressing information that are captured, without notice or consent, when they access and view the Website. These privacy interests are recognized by the California Constitution, CDAFA, CIPA, HIPAA, and numerous other statutes.

171. Plaintiff and Class members had a reasonable expectation of privacy under the circumstances, as they could not have reasonably expected that Defendant would violate state and federal privacy laws. Plaintiff and Class members were not aware of and could not have reasonably expected that Defendant would use website tracking technology and install third-party tracker cookies without notice or obtaining consent. Those unauthorized Trackers collected and transmitted to undisclosed third parties Plaintiff's and Class members' communications and personally identifying and addressing information, including their IP addresses, which contain geolocation data.

172. Defendant's unauthorized (1) installation of the Trackers and (2) collection and disclosure to third parties of Plaintiff's and Class members' communications and personally identifying and addressing information, all without consent or adequate notification to Plaintiff and Class members, are an invasion of Plaintiff's and Class members' privacy.

173. Defendant's conduct constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that (i) the information disclosed by Defendant and shared with third-party trackers was personally identifying information protected by the California Constitution and numerous California and federal statutes; (ii) Defendant did not have authorization or consent to disclose those communications and personally identifying and addressing information, including IP addresses, to any third-party tracker embedded in the Website, and the Trackers did not have

authorization to collect and use that information; and (iii) the invasion deprived Plaintiff and Class members of the ability to control the dissemination and circulation of that information, an ability that is considered a fundamental privacy right. Defendant's conduct constitutes a severe and egregious breach of social norms.

174. As a direct and proximate result of Defendant's actions, Plaintiff and Class members have had their privacy invaded and have sustained injury, including injury to their peace of mind.

175. Plaintiff and the Class members seek appropriate relief for that injury, including but not limited to restitution, disgorgement of profits earned by Defendant as a result of or in connection with the intrusions upon Plaintiff's and Class members' privacy, nominal damages, and any and all other equitable relief that will compensate Plaintiff and Class members properly for the harm to their privacy interests.

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

FIFTH CAUSE OF ACTION

(Violations of the CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code §17200, *et seq.*)

177. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

178. Violated California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, et seq., by engaging in unlawful, unfair, or fraudulent business acts and practices that constitute "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. by violating the provisions of the CIPA prohibiting unauthorized wiretapping, Cal. Pen. Code § 631, *et. seq*.;

b. by violating the provisions of the ECPA prohibiting unauthorized wiretapping, 18 U.S.C 2510, *et. seq*.;

c. by violating the provisions of the CIPA prohibiting unauthorized trap and trace, Cal. Pen. Code § 638.51;

d. by violating the CDAFA, Cal. Pen. Code § 502, *et. seq.;*

179. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous,

unconscionable, and/or substantially injurious to Plaintiff. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities do not share, collect, or transmit data without consumer consent, as reflected by laws like the CIPA, Cal. Penal Code §§ 631 & 632, the CDAFA, Cal. Penal Code § 502, *et seq*.; the California Trap and Trace Law, Cal. Penal Code § 638.51; and the ECPA, 18 U.S.C. § 2510, *et. seq*.

180. Moreover, these acts and practices are fraudulent in contrary to California law, and Plaintiff and the Class are entitled to a reasonable expectation that Defendant would only act in compliance with the substantive law.

181. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiffs were injured and lost money or property, including but not limited to the loss of their legally protected interest in the privacy of their personal information, data, and communications. In addition, Defendant treated the personal information, data, and communications of Plaintiffs as its own property, and sold and/or otherwise used it for profit, causing a loss of money and property to Plaintiffs.

182. In addition to the losses described above, Defendant's unfair, unlawful, and fraudulent business practices above have taken money or property in the value of the information stolen from Plaintiff and the Class. Similar information, as provided in focus groups, would entitle Plaintiff and the Class Members to compensation in the amount of $50 to $200.

183. Defendant knew or should have known that its sale of information to unauthorized third parties would violate the CIPA, ECPA, and CDAFA. Defendant's actions in engaging in the above-named unfair practice and deceptive acts were intentional, knowing, and willful, and/or wanton and reckless with respect to the rights of the Plaintiffs.

184. Plaintiffs seek relief under the UCL, including restitutionary disgorgement of all monies withheld, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. P. § 1021.5), and injunctive or other equitable relief.

DEMAND FOR JURY TRIAL

185. Plaintiff and the Class hereby demand trial by jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendants as follows:

1. For an order certifying the Class, naming Plaintiff as the representatives of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;
2. For an order declaring that Defendant's conduct violates the statutes referenced herein;
3. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
4. For statutory damages of $5,000 for each violation of CIPA section 631 and 638.51(a);
5. For statutory damages of $10,000 for each violation of the Federal Wiretap Act;
6. For pre- and post-judgment interest on all amounts awarded;
7. For an order of restitution and all other forms of equitable monetary relief; and
8. For an order providing injunctive and other equitable relief as necessary to protect the Plaintiff's interests as requested herein, including, but not limited to:
    a. Ordering that Defendant immediately cease and desist the unauthorized interception, transfer, release, sale, and disclosure of Plaintiffs' data;
    b. Ordering that Defendant remove, block, disable, control, update, manage, and audit any code, software, hardware, operations, systems, policy, procedure, protocols, and processes that allow all unauthorized third parties to intercept, access, copy, collect, take, open, view, monitor, mine, analyze, store, sell, gain, exchange, or otherwise use Plaintiffs' data;
    c. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner data not necessary for its provision of services.
9. For an order awarding and the Class their reasonable attorney's fees and expenses and costs of suit.

Dated: June 30, 2026

POTTER HANDY LLP

By: _____

James M. Treglio, Esq.
Mark Potter, Esq.
Isabel Rose Masanque, Esq.
Attorneys for Plaintiffs