UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AARON DEIVAPRAKASH, individually and on behalf of all others similarly situated, Plaintiff, v. CONDÉ NAST DIGITAL, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Aaron Deivaprakash ("Plaintiff"), individually and on behalf of all others 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. Defendant Condé Nast Digital ("Defendant") owns and operates the websites newyorker.com (the "New Yorker Website") and wired.com (the "Wired Website") (collectively, the "Websites").

2. When users visit the Websites, Defendant causes three Trackers—the DoubleClick Tracker, Audiencerate Tracker, and AGKN Tracker (collectively, the "Trackers")—to be installed on the Website visitors' internet browsers. Defendant then uses these Trackers to collect Website visitors' IP addresses.

3. Because the Trackers capture Website visitors' "routing, addressing, or signaling information," each Tracker constitute a "pen register" under Section 638.50(b) of the California Invasion of Privacy Act ("CIPA"). Cal. Penal Code § 638.50(b).

4. 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 CIPA section 638.51.

PARTIES

6. Plaintiff Deivaprakash resides in Dublin, California and has an intent to remain there, and is therefore a citizen of California. Plaintiff Deivaprakash was in California when he visited the Website.

7. Defendant Condé Nast Digital is a New York corporation with its principal place of business in New York, New York.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(a) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00 exclusive of interest and costs, there are over 100 members of the putative class, and at least one class member is a citizen of a different state than Defendant.

9. This Court has specific jurisdiction over Defendant because Defendant is incorporated and maintains its principal place of business in New York.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant resides in this District.

FACTUAL ALLEGATIONS

I. THE CALIFORNIA INVASION OF PRIVACY ACT

11. 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.

12. As relevant here, 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."

13. A "pen register" is "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).

14. 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).

15. 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.

16. 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.

17. For example, if a user sends an email, a "pen register" might record the email address it was sent from, the email address 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.

18. 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. Sep. 26, 2013); *see also Greenley v. Kochava, Inc.*, 2023 WL 4833466, at *15 (S.D. Cal. July 27, 2023) (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).

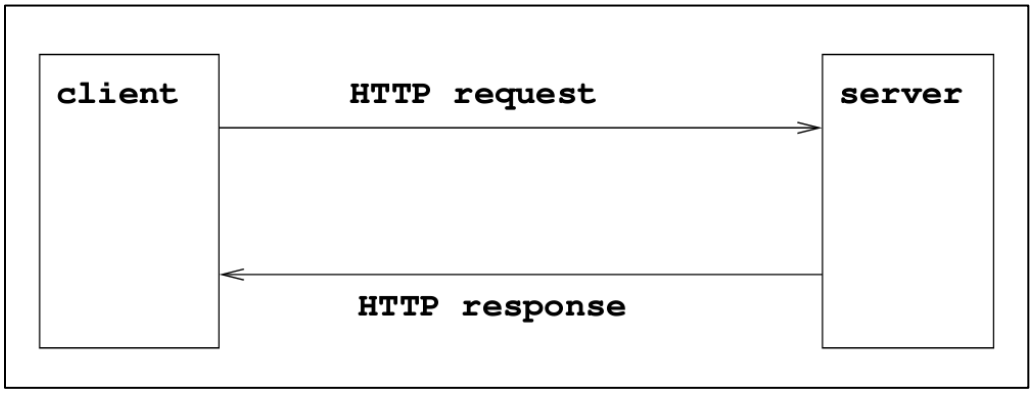
19. Individuals may bring an action against the violator of any provision of CIPA—including CIPA section 638.51—for $5,000 per violation. Cal. Penal Code § 637.2(a)(1).

II. DEFENDANT VIOLATES THE CALIFORNIA INVASION OF PRIVACY ACT

A. The Trackers Are "Pen Registers"

20. To make Defendant's Websites load on a user's internet browser, the browser sends an "HTTP request" or "GET" request to Defendant's server where the relevant Website data is stored. In response to the request, Defendant's server sends an "HTTP response" back to the browser with a set of instructions. A general diagram of this process is pictured at Figure 1, which explains how Defendant's Websites transmit instructions back to users' browsers in response to HTTP requests. *See* Figure 1.

Figure 1:



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

22. In addition, the server's instructions cause the Trackers to be installed on a user's browser. The Trackers then cause the browser to send identifying information—including the user's IP address—to Google, Audiencerate, and Neustar.

23. 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).

24. Thus, the IP address enables a device to communicate with another device—such as a computer's browser communicating with a server—and the IP address contains geographical location.

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

26. Much like a telephone number, an IP address is a unique numerical code associated with a specific internet-connected device. Thus, knowing a user's IP address—and therefore geographical location—"provide[s] a level of specificity previously unfound in marketing."[1]

27. An IP address allows advertisers to (i) "[t]arget [customers by] countries, cities, neighborhoods, and … postal code"[2] and (ii) "to target specific households, businesses[,] and even individuals with ads that are relevant to their interests."[3] Indeed, "IP targeting is one of the most targeted marketing techniques [companies] can employ to spread the word about [a] product or service"[4] *because* "[c]ompanies can use an IP address … to personally identify individuals."[5]

28. 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

[1] *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA (Nov. 20, 2023) https://www.accudata.com/blog/ip-targeting/.

[2] *Location-based Targeting That Puts You in Control*, CHOOZLE, https://choozle.com/geotargeting-strategies/.

[3] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf.

[4] *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA (Nov. 20, 2023), https://www.accudata.com/blog/ip-targeting/.

[5] Trey Titone, *The future of IP address as an advertising identifier*, AD TECH EXPLAINED (May 16, 2022), https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/.

college-wide Wi-Fis.[6] Or, for a job fair in specific city, companies can send advertisements to only those in the general location of the upcoming event.[7]

29. 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."[8] "By targeting specific households or businesses, businesses can avoid wasting money on ads that are unlikely to be seen by their target audience."[9]

30. In addition, "IP address targeting can help businesses to improve their overall marketing strategy."[10] "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."[11]

31. As alleged below, Defendant installs each of the Trackers on the user's browser for marketing and analytics purposes, and the Trackers collect information—users' IP addresses—that identifies the outgoing "routing, addressing, or signaling information" of the user. Accordingly, the Trackers are each "pen registers."

---

[6] *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA (Nov. 20, 2023), https://www.accudata.com/blog/ip-targeting/.

[7] *See*, *e.g.*, *Personalize Your Website And Digital Marketing Using IP Address*, GEOFLI, https://geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-marketing-campaigns.

[8] Herbert Williams, *The Benefits of IP Address Targeting for Local Business*es, LINKEDIN (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf.

[9] *Id.*

[10] *Id.*

[11] *Id.*

1. DoubleClick Tracker on the New Yorker Website

32. The Google Marking Platform is a software-as-a-service offered by Google that develops the DoubleClick Tracker, which it provides to website owners like Defendant for a fee.

33. According to Google, its marketing platform is "an integrated ad technology platform that enables advertisers to more effectively create, manage and grow high-impact digital marketing campaigns. DDM [DoubleClick Digital Marketing] brings together world-class solutions to help buyers run holistic programs across multiple channels."[12]

34. In other words, Google enables companies to sell advertising space on their websites, thereby earning revenue, and allows companies to place advertisements on other companies' websites, thereby driving brand awareness and sales. To achieve this, Google uses its DoubleClick Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant's New Yorker Website.

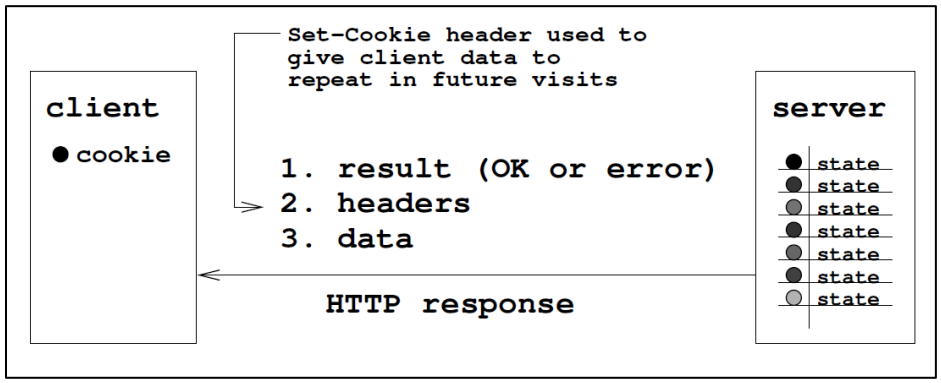
35. The first time a user visits Defendant's New Yorker Website, the user's browser sends an HTTP request to Defendant's server, and Defendant's server sends an HTTP response with directions to install the DoubleClick Tracker on the user's browser. The DoubleClick Tracker, in turn, instructs the user's browser to send Google the user's IP address.

36. Moreover, Google stores a cookie with the user's IP address in the user's browser cache. When the user subsequently visits Defendant's New Yorker Website, the DoubleClick Tracker locates the cookie identifier stored on the user's browser. If the cookie is stored on the browser, the DoubleClick Tracker causes the browser to send the cookie along with the user's IP address to Google. A general diagram of this process is pictured as Figure 2, which explains how

[12] *DoubleClick Digital Marketing*, GOOGLE HELP, https://support.google.com/faqs/answer/2727482?hl=en#:~:text=DoubleClick%20Search:%20A%20search%20management,reporting%20on%20rich%20media%20advertising

the New Yorker Website causes the DoubleClick Tracker to install a cookie on the user's browser and instructs the user's browser to send the user's IP address through the cookie. *See* Figure 2.

Figure 2:



37. If the user clears his or her cookies, then the user wipes out the DoubleClick Tracker from its cache. Accordingly, the next time the user visits Defendant's New Yorker Website the process begins over again: (i) Defendant's server installs the DoubleClick Tracker on the user's browser, (ii) the DoubleClick Tracker instructs the browser to send Google the user's IP address, (iii) the DoubleClick Tracker stores a cookie in the browser cache, and (iv) Google will continue to receive the user's IP address on subsequent New Yorker Website visits as part of the cookie transmission. *See* Figure 3.

//

//

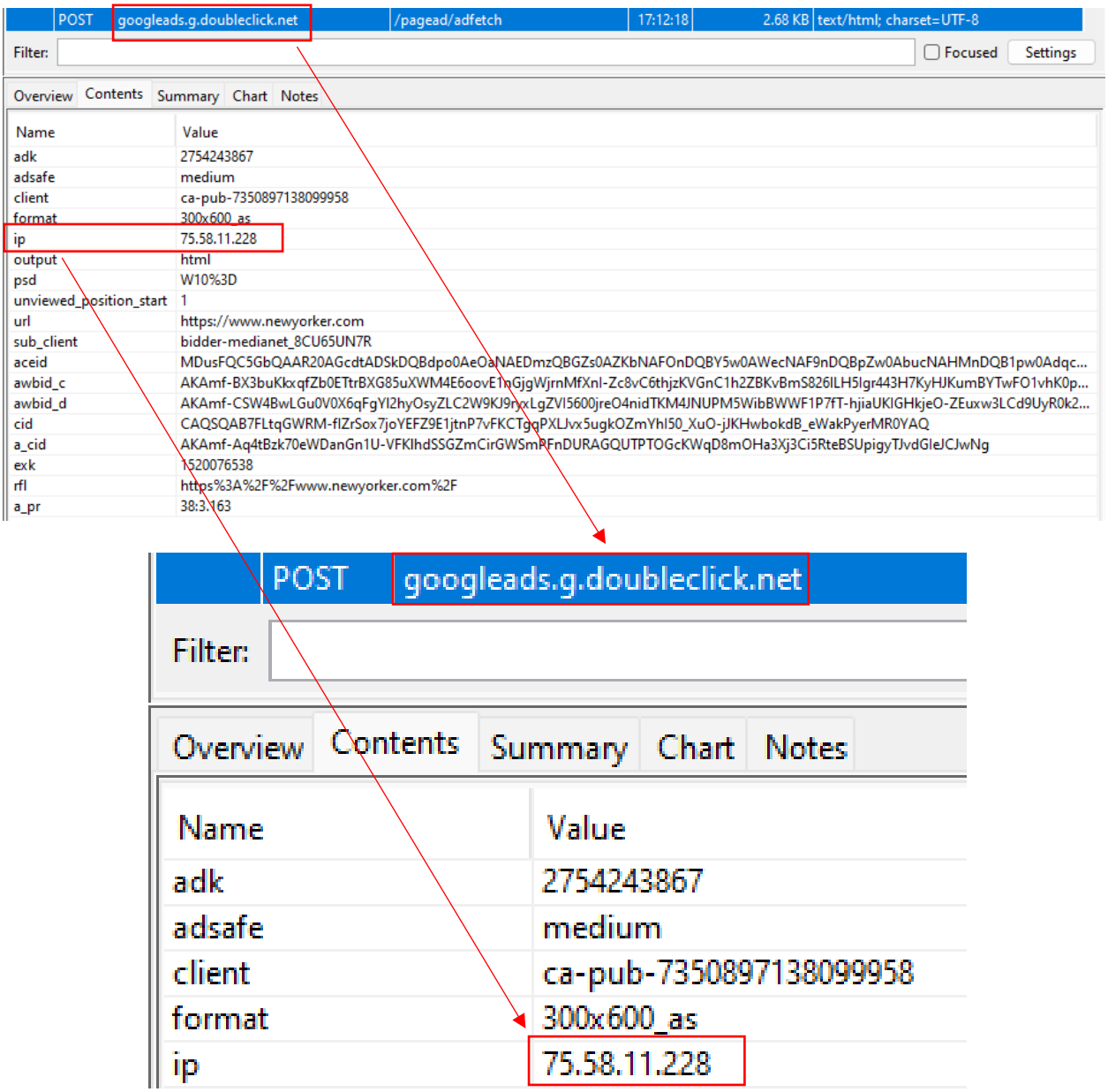
//

//

//

//

Figure 3:



38. The DoubleClick Tracker is at least a "process" because it is "software that identifies consumers, gathers data, and correlates that data." *Greenley*, 2023 WL 4833466, at *15.

39. Further, the DoubleClick Tracker is a "device" because "in order for software to work, it must be run on some kind of computing device." *See*, *e.g.*, *James v. Walt Disney Co.*, --- F. Supp. 3d ---, 2023 WL 7392285, at *13 (N.D. Cal. Nov. 8, 2023).

40. Because the DoubleClick Tracker captures the outgoing information—the IP address—from visitors to websites, it is a "pen register" for the purposes of CIPA section 638.50(b).

2. Audiencerate Tracker on the Wired Website

41. Audiencerate LTD ("Audiencerate") is a software-as-a-service company that develops the Audiencerate Tracker, which it provides to website owners, like Defendant for a fee.

42. According to Audiencerate, it "enable[s] data-driven advertising via [its] proprietary technology and platforms."[13]

43. "One side of [Audiencerate's] business is dedicated to helping data owners monetize their data and license audiences in the world's largest programmatic media buying marketplaces. The other side provides targeting data to marketers, enabling them to model and target audiences with more complexity and sophistication."[14]

44. Just like Google, Audiencerate uses its Tracker to receive, store, and analyze data sent collected from website visitors, such as visitors of Defendant's Website.

45. In other words, Audiencerate enables companies to sell advertising space on their websites, thereby earning revenue, and allows companies to place advertisements on other companies' websites, thereby driving brand awareness and sales. To achieve this, Audiencerate uses its Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant's Wired Website.

46. Similar to above, the first time a user visits Defendant's Wired Website, the user's browser sends an HTTP request to Defendant's server, and Defendant's server sends an HTTP

[13] AUDIENCERATE, https://www.audiencerate.com/

[14] *AWS Enables Audiencerate to Process Over a Billion Requests per Week*, AWS (2020), https://aws.amazon.com/solutions/case-studies/audiencerate-case-study/.

response with directions to install the Audiencerate Tracker on the user's browser. The Audiencerate Tracker, in turn, instructs the user's browser to send Audiencerate the user's IP address.

47. Moreover, Audiencerate stores a cookie with the user's IP address in the user's browser cache. When the user subsequently visits Defendant's Wired Website, the Audiencerate Tracker locates the cookie identifier stored on the user's browser. If the cookie is stored on the browser, the Audiencerate Tracker causes the browser to send the cookie along with the user's IP address to Audiencerate. A general diagram of this process is pictured as Figure 2, which explains how the Website causes the Audiencerate Tracker to install a cookie on the user's browser instructs the user's browser to send the user's IP address through the cookie. *See* Figure 2, *supra*.

48. If the user clears his or her cookies, then the user wipes out the Audiencerate Tracker from its cache. Accordingly, the next time the user visits Defendant's Wired Website the process begins over again: (i) Defendant's server installs the Audiencerate Tracker on the user's browser, (ii) the Audiencerate Tracker instructs the browser to send Audiencerate the user's IP address, (iii) the Audiencerate Tracker stores a cookie in the browser cache, and (iv) Audiencerate will continue to receive the user's IP address on subsequent Wired Website visits as part of the cookie transmission. *See* Figure 4.

//

//

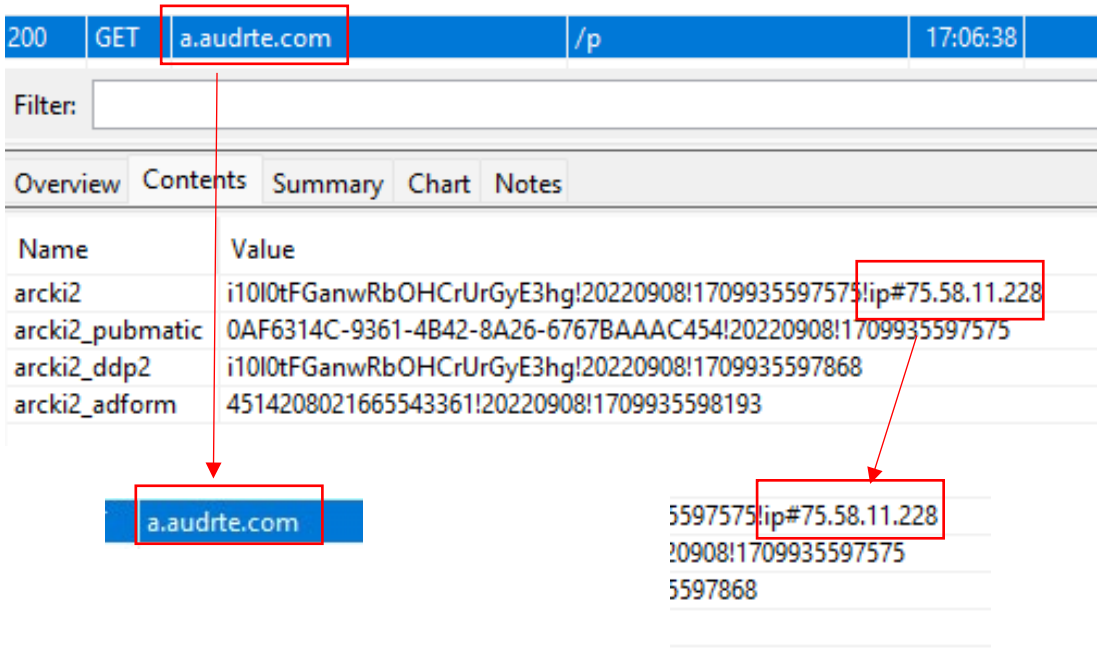
//

//

//

//

Figure 4:



49. The Audiencerate Tracker is at least a "process" because it is "software that identifies consumers, gathers data, and correlates that data." *Greenley*, 2023 WL 4833466, at *15.

50. Further, the Audiencerate Tracker is a "device" because "in order for software to work, it must be run on some kind of computing device." *James*, --- F. Supp. 3d ---, 2023 WL 7392285, at *13.

51. Because the Audiencerate Tracker captures the outgoing information—the IP address—from visitors to websites, it is a "pen register" for the purposes of CIPA section 638.50(b).

3. AGKN Tracker on the Wired Website

52. Neustar is a software-as-a-service company that develops the AGKN Tracker, which it provides to website owners like Defendant for a fee.

53. According to Neustar, the company "[t]ransform[s] omnichannel media performance with the next generation of identity-driven marketing capabilities."[15]

54. In other words, Neustar enables companies to sell advertising space on their websites, thereby earning revenue, and allows companies to place advertisements on other companies' websites, thereby driving brand awareness and sales. To achieve this, Neustar uses its Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant's Wired Website.

55. Similar to above, the first time a user visits Defendant's Wired Website, the user's browser sends an HTTP request to Defendant's server, and Defendant's server sends an HTTP response with directions to install the AGKN Tracker on the user's browser. The AGKN Tracker, in turn, instructs the user's browser to send Neustar the user's IP address.

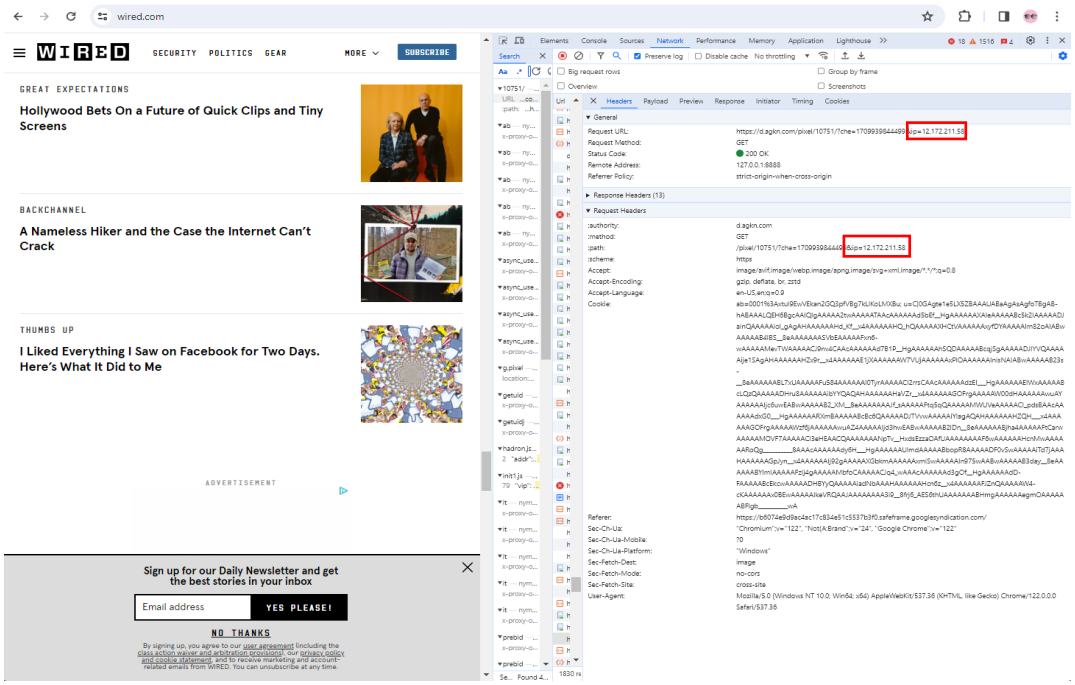
56. Moreover, Neustar stores a cookie with the user's IP address in the user's browser cache. When the user subsequently visits Defendant's Wired Website, the AGKN Tracker locates the cookie identifier stored on the user's browser. If the cookie is stored on the browser, the AGKN Tracker causes the browser to send the cookie along with the user's IP address to Neustar. A general diagram of this process is pictured as Figure 2, which explains how the Website causes the AGKN Tracker to install a cookie on the user's browser instructs the user's browser to send the user's IP address through the cookie. *See* Figure 2, *supra*.

57. If the user clears his or her cookies, then the user wipes out the AGKN Tracker from its cache. Accordingly, the next time the user visits Defendant's Wired Website the process begins over again: (i) Defendant's server installs the AGKN Tracker on the user's browser, (ii) the AGKN Tracker instructs the browser to send Neustar the user's IP address, (iii) the AGKN Tracker

[15] *TruAudience,* TRANSUNION, https://www.transunion.com/solution/truaudience

stores a cookie in the browser cache, and (iv) Neustar will continue to receive the user's IP address on subsequent Wired Website visits as part of the cookie transmission. *See* Figure 5.

Figure 5:



58. The AGKN Tracker is at least a "process" because it is "software that identifies consumers, gathers data, and correlates that data." *Greenley*, 2023 WL 4833466, at *15.

59. Further, the AGKN Tracker is a "device" because "in order for software to work, it must be run on some kind of computing device." *James*, --- F. Supp. 3d ---, 2023 WL 7392285, at *13.

60. Because the AGKN Tracker captures the outgoing information—the IP address—from visitors to websites, it is a "pen register" for the purposes of CIPA section 638.50(b).

B. Defendant Installed And Used The Trackers On Plaintiff's And Users' Browsers Without Prior Consent Or A Court Order

61. Defendant owns and operates the Websites.

62. The New Yorker Website is "a daily source of news and cultural coverage, plus an expansive audio division, an award-winning film-and-television arm, and a range of live events featuring people of note."[16] The Website provides news on books & culture, fiction & poetry, humor & cartoons, magazine, puzzle & games, video, podcasts, etc.

63. The Wired Website "illuminates how technology is changing every aspect of our lives—from culture to business, science to design."[17] The Website provides news on security, politics, business, science, and culture.

64. When companies build their websites, they install or integrate various third-party scripts into the code of the website in order to collect data from users or perform other functions.[18]

[16] *About Us*, NEWYORKER https://www.newyorker.com/about/us

[17] *Frequently Asked Questions*, WIRED, https://www.wired.com/about/faq/

[18] *See Third-party Tracking*, PIWIK, https://piwik.pro/glossary/third-party-tracking/ ("Third-party tracking refers to the practice by which a tracker, other than the website directly visited by the user, traces or assists in tracking the user's visit to the site. Third-party trackers are snippets of code that are present on multiple websites. They collect and send information about a user's browsing history to other companies…").

65. Often times, third-party scripts are installed on websites "for advertising purposes."[19]

66. Further, "[i]f the same third-party tracker is present on many sites, it can build a more complete profile of the user over time."[20]

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

68. As outlined above, when a user visits the Websites, the Websites' code—as programmed by Defendant—installs the Trackers onto the user's browser.

69. Upon installing the Trackers on its Websites, Defendant uses the Trackers to collect the IP address of visitors to the Websites, including the IP address of Plaintiff and Class Members. *See* Figure 3 (DoubleClick Tracker), Figure 4 (Audiencerate Tracker), and Figure 5 (AGKN Tracker), *supra*.

70. Defendant then uses the IP address of Website visitors, including those of Plaintiff and Class Members, to serve targeted advertisements and conduct website analytics.

71. At no time prior to the installation and use of the Trackers on Plaintiff's and Class Members's browsers, or prior to the use of the Trackers, did Defendant procure Plaintiff's and Class Members's consent for such conduct. Nor did Defendant obtain a court order to install or use the Trackers.

---

[19] *Id*.

[20] *Id*.

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

72. The collection of Plaintiff's and Class Members' personally identifying, non-anonymized information through Defendant's installation and use of the Trackers constitutes an invasion of privacy.

73. 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.

1. Defendant Uses The DoubleClick Tracker For The Purposes Of Marketing, Advertising, And Analytics On The New Yorker Website

74. Google describes its marketing platform as "an integrated ad technology platform that enables advertisers to more effectively create, manage and grow high-impact digital marketing campaigns. DDM [DoubleClick Digital Marketing] brings together world-class solutions to help buyers run holistic programs across multiple channels."[21]

75. Google helps companies like Defendant market, advertise, and analyze user data from its website. Specifically, the Google Marketing Platform allows companies to gain a "deeper understanding of [] [their] customers and identify [] their most valuable audiences."[22] This is done by utilizing first and third-party data.

76. For example, Google enables websites, such as Defendant, to buy and sell advertisement spaces on their web pages through features like Google's Bid Manager, which helps "agencies and advertisers buy online advertising across ad exchanges, on an impression-by-

[21] *DoubleClick Digital Marketing*, GOOGLE HELP, https://support.google.com/faqs/answer/2727482?hl=en#:~:text=DoubleClick%20Search:%20A%20search%20management,reporting%20on%20rich%20media%20advertising

[22] *Marketing Platform*, GOOGLE, https://marketingplatform.google.com/about/enterprise/

impression basis, in real time."[23]. To ensure that an effective advertisement is shown to the consumer, the publisher shares data about the user with Google and Google serves the targeted ad.

77. When users visit Defendant's New Yorker Website, Google collects users' IP addresses through its DoubleClick Tracker so that Defendant can analyze user data, create and analyze the performance of marketing campaigns, and target specific users or specific groups of users for advertisements. All of this helps Defendant further monetize its New Yorker Website and maximize revenue by collecting and disclosing user information.

2. Defendant Uses The Audiencerate Tracker For The Purposes Of Marketing, Advertising, And Analytics On The Wired Website

78. Audiencerate is a data platform that helps "distribute anonymously personally identifiable information-based and device-based segment data" for marketing, advertising, and analysis purposes.[24]

79. Companies such as Defendant share their users' data with Audiencerate through "daily synchronization" via the Audiencerate Tracker.[25] Audiencerate claims to anonymize the data and organizes it into segments.[26] Then, companies use the segmented data to run targeted campaigns and perform data analysis through Audiencerate's platform.[27] *See* Figure 8.

[23] *DoubleClick Digital Marketing*, GOOGLE HELP, https://support.google.com/faqs/answer/2727482?hl=en#:~:text=DoubleClick%20Search:%20A%20search%20management,reporting%20on%20rich%20media%20advertising.

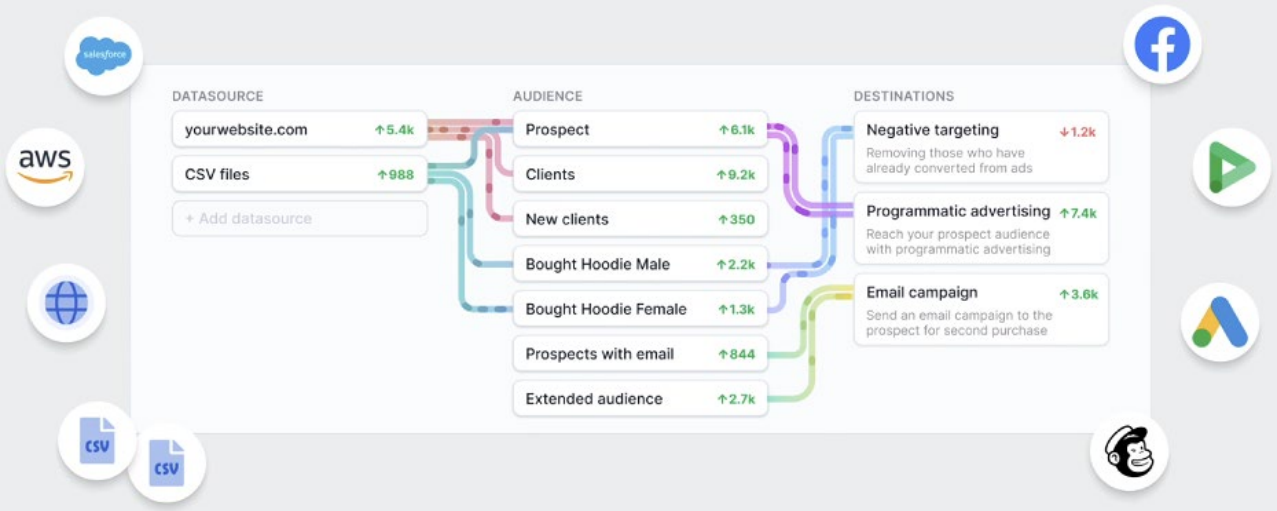
[24] *Product Overview*, AUDIENCERATE, https://app.audiencerate.com/doc/home

[25] AUDIENCERATE, https://www.audiencerate.com/

[26] *Product Overview*, AUDIENCERATE, https://app.audiencerate.com/doc/home

[27] *Id.*

Figure 8:



80. In addition to helping companies make better use of their own customer data, Audiencerate helps companies *sell* their customers' data to further "monetize data."[28]

81. In order to perform the functions listed above, Audiencerate needs to collect data that identifies a particular user. This is why Audiencerate collects IP addresses: it allows Audiencerate to segment users in order to run targeted campaigns and perform data analysis.

82. In other words, companies like Defendant are collecting users' data and sending it to Audiencerate for a profit, whether it is by optimizing marketing campaigns or by purely selling the data.

83. In order to perform the functions listed above, Audiencerate needs to collect data that identifies a particular user. This is why Audiencerate collects IP addresses: it allows Audiencerate to ascertain a user's location and target that user with advertisements tailored to their

[28] *Audiencerate partnership sees Sirdata integrated on Adform marketplace for the first time*, SIRDATA (Dec. 10, 2020), https://news.sirdata.com/en/press-release-audiencerate-sirdata-partnership/

location, as well as to track a user's Website activity over time (*i.e.*, through repeated Website visits) to target a user with advertisements relevant to the user's personal browsing activity.

84. In other words, when users visit Defendant's Wired Website, Audiencerate collects users' IP addresses through its Audiencerate Tracker so that Defendant can analyze user data, create and analyze the performance of marketing campaigns, and target specific users or specific groups of users for advertisements. All of this helps Defendant further monetize its Wired Website and maximize revenue by collecting and disclosing user information.

3. Defendant Uses The AGKN Tracker For The Purposes Of Marketing, Advertising, And Analytics On The Wired Website

85. Neustar is a digital advertising platform that helps companies like Defendant market, advertise, and analyze user data from its website.

86. According to Neustar, it "powers data-driven marketing and measurement with a suite of privacy-first identity resolution, data enrichment, audience targeting and advanced analytics solutions."[29]

87. Similar to above, Neustar enables advertisers to target specific people. This is done through their TruAudience Identity Solutions, which "[t]ransform omnichannel marketing and media performance with the next generation of identity resolution capabilities." [30] This service helps "[r]educe media waste and off-target advertising by deduplicating identities and removing

[29] *TruAudience*, TRANSUNION, https://www.transunion.com/solution/truaudience

[30] *TruAudience Identity Solutions*, TRANSUNION, https://www.transunion.com/solution/truaudience/identity

incorrect information."[31] Neustar boasts that this "real-time identity management" helps websites, like Defendant, have "10x [r]eturn on your investment in your solution."[32]

88. Neustar collects data to use for targeted marketing. For example, Neustar "[c]onnects known and unknown consumer data – across devices, households and channels."[33]

89. In order to perform the functions listed above, Neustar needs to collect data that identifies a particular user. This is why Neustar collects IP addresses: it allows Neustar to ascertain a user's location and target that user with advertisements tailored to their location, as well as to track a user's Website activity over time (*i.e.*, through repeated Website visits) to target a user with advertisements relevant to the user's personal browsing activity.

90. In other words, companies like Defendant are collecting users' data and sending it to Neustar for a profit, whether it is by optimizing marketing campaigns or by purely selling the data.

91. When users visit Defendant's Website, Neustar collects users' IP addresses through its AGKN Tracker so that Defendant can analyze user data, create and analyze the performance of marketing campaigns, and target specific users or specific groups of users for advertisements. All of this helps Defendant further monetize its Website and maximize revenue by collecting and disclosing user information.

---

[31] *Id.*

[32] *Id.*

[33] *TruAudience Identity Solutions*, TRANSUNION, https://www.transunion.com/solution/truaudience/data-collaboration

PLAINTIFF'S EXPERIENCE

92. Plaintiff has visited the Websites on his desktop browser multiple times—as recent as March 2024 and as long ago as 2012—and has done so throughout the entirety of the class period.

93. When Plaintiff visited the Websites, the Websites' code—as programmed by Defendant—caused the Trackers to be installed on Plaintiff's browser. Defendant, Google, and Audiencerate then used the Trackers to collect Plaintiff's IP address. *See* Figures 3-4.

94. Defendant, Google, and Audiencerate used the information collected by the Trackers to analyze Website data and marketing campaigns, conduct targeted advertising based on Plaintiff's location, and ultimately boost Defendant's and advertisers' revenue.

95. Plaintiff did not provide his prior consent to Defendant to install or use the Trackers on Plaintiff's browser.

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

97. Plaintiff has, therefore, had his privacy invaded by Defendant's violations of CIPA § 638.51(a).

98. Although Defendant utilizes at least three different Trackers on the Website (DoubleClick, Audiencerate, and AGKN), they all operate in the same manner and perform the same function, *i.e.*, collecting Plaintiff's and Class members' IP addresses. 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.

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

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

101. Thus, like Plaintiff, Class Members have also had their privacy invaded by Defendant's violations of CIPA § 638.51(a).

CLASS ALLEGATIONS

102. Pursuant to Fed. R. Civ. P. Rule 23, Plaintiff seeks to represent a class defined as all California residents who accessed the Websites in California and had their IP address collected by the Trackers (the "Class").

103. The following people are excluded from the Class: (i) any Judge presiding over this action and members of her or her family; (ii) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or their parents have a controlling interest (including current and former employees, officers, or directors); (iii) persons who properly execute and file a timely request for exclusion from the Class; (iv) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (v) Plaintiff's counsel and Defendant's counsel; and (vi) the legal representatives, successors, and assigns of any such excluded persons.

104. **Numerosity:** The number of people within the Class is substantial and believed to amount to thousands, if not millions of persons. It is, therefore, impractical to join each member of the Class as a named plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class renders 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 Class is ascertainable and identifiable from Defendant's records.

105. **Commonality and Predominance:** There are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions

affecting only individual members of the Class. These common legal and factual questions, which do not vary between members of the Class, and which may be determined without reference to the individual circumstances of any Class Member, include, but are not limited to, the following:

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

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

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

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

(e) Whether Plaintiff and members of the Class are entitled to actual and/or statutory damages for the aforementioned violations.

106. **Typicality:** The claims of the named Plaintiff are typical of the claims of the Class because the named Plaintiff, like all other members of the Class Members, visited the Websites and had his IP address collected by the Trackers, which were installed and used by Defendant.

107. **Adequate Representation:** Plaintiff is an adequate representative of the Class 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 Class will be fairly and adequately protected by Plaintiff and his counsel.

108. **Superiority:** The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of members of the Class. Each individual member of the Class 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.

CAUSES OF ACTION

COUNT I
Violation Of The California Invasion Of Privacy Act, Cal. Penal Code § 638.51(a)

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

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

111. 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."

112. 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).

113. 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).)

114. 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 Plaintiff's and Class Members' IP addresses.

115. The Trackers do not collect the content of Plaintiff's and the Class's electronic communications with the Websites. *In re Zynga Privacy Litig.,* 750 F.3d 1098, 1108 (9th Cir. 2014) ("IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication…") (cleaned up).

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

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

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

PRAYER FOR RELIEF

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

(a) For an order certifying the Class, naming Plaintiff as the 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) For statutory damages of $5,000 for each violation of CIPA § 638.51(a);

(e) For pre- and post-judgment interest on all amounts awarded;

(f) For an order of restitution and all other forms of equitable monetary relief; and

(g) For an order awarding and the Class their reasonable attorney's fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of any and all issues in this action so triable of right.

Dated: August 28, 2024

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Yitzchak Kopel*
Yitzchak Kopel

Yitzchak Kopel
Alec M. Leslie
Max S. Roberts
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: ykopel@bursor.com
aleslie@bursor.com
mroberts@bursor.com

Attorneys for Plaintiff

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: Class Action Lawsuit Alleges The New Yorker, Wired Secretly Collect Website Users' IP Addresses

---