UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CHIH-YUAN CHANG, individually and on behalf of all others similarly situated, Plaintiff, v. BUZZFEED, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Chih-Yuan Chang ("Plaintiff"), individually and on behalf of all others similarly situated, by and through her attorneys, makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to allegations specifically pertaining to herself and her counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. Buzzfeed, Inc. ("Defendant" or "Buzzfeed") owns and operates a news and entertainment website, buzzfeed.com (the "Website").

2. When users visit the Website, Defendant causes three Trackers—the Sharethrough Tracker, IQM Tracker, and Dotomi Tracker (collectively, the "Trackers")—to be installed on Website visitors' internet browsers. Each of these Trackers collects Website visitors' IP addresses.

3. Because the Trackers capture Website visitors' "routing, addressing, or signaling information," the Trackers each constitute a "pen register" under Section 638.50(b) of the California Invasion of Privacy Act ("CIPA"). Cal. Penal Code § 638.50(b); *see also Greenley v. Kochava, Inc.*, 2023 WL 4833466 (S.D. Cal. July 27, 2023).

4. By installing and using these Trackers without Plaintiff's prior consent and without a court order, Defendant violated CIPA § 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 § 638.51.

PARTIES

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

7. Defendant Buzzfeed is a Delaware corporation with its principal place of business at 111 East 18th Street, New York, New York 10003.

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 state different than Defendant.

9. This Court has general personal jurisdiction over Defendant because Defendant has its principal place of business in New York City, New York.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) 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 § 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 "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. Sept. 26, 2013); *see also Greenley*, 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).

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

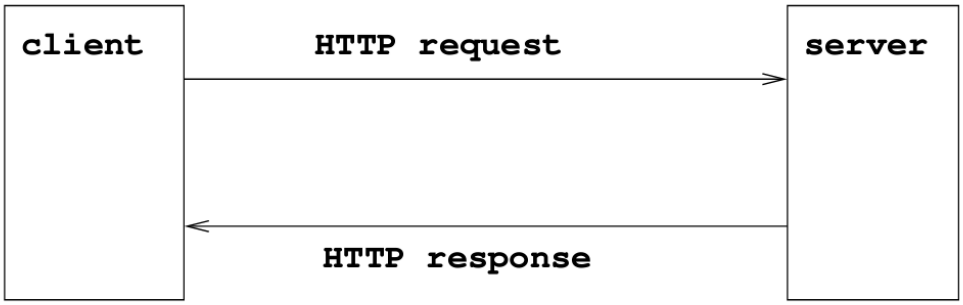
II. DEFENDANT VIOLATES THE CALIFORNIA INVASION OF PRIVACY ACT

A. The Trackers Are "Pen Registers"

20. To make Defendant's Website 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. *See* Figure 1.

Figure 1:



21. 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.

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

23. The 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 specific 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 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

---

[1] *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA, https://www.accudata.com/blog/ip-targeting/ (last visited April 1, 2024).

[2] *Location-based Targeting That Puts You in Control*, CHOOZLE, https://choozle.com/geotargeting-strategies/ (last visited April 1, 2024).

[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, https://www.accudata.com/blog/ip-targeting/ (last visited April 1, 2024).

[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/.

[6] *See*, *e.g.*, *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA, https://www.accudata.com/blog/ip-targeting/ (last visited April 1, 2024).

[7] *See*, *e.g.*, *Personalize Your Wesbite And Digiital Marketing Using IP Address*, GEOFLI, https://geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-marketing-campaigns (last visited April 1, 2024).

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 the Trackers on the user's browser for marketing and analytics purposes, and the Trackers collect information—users' IP addresses as well as other information—that identifies the outgoing "routing, addressing, or signaling information" of the user. Accordingly, the Trackers are "pen registers."

1. Sharethrough Tracker

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

33. According to Sharethrough, it is "building a sustainable advertising ecosystem for journalists, content creators and app developers, by connecting publishers and advertisers with true technology innovation supporting all omnichannel formats including display, video & native, devices, and user experiences."[12]

34. In other words, Sharethrough enables companies to sell advertising space on their

---

[8] 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.

[9] *Id.*

[10] *Id.*

[11] *Id.*

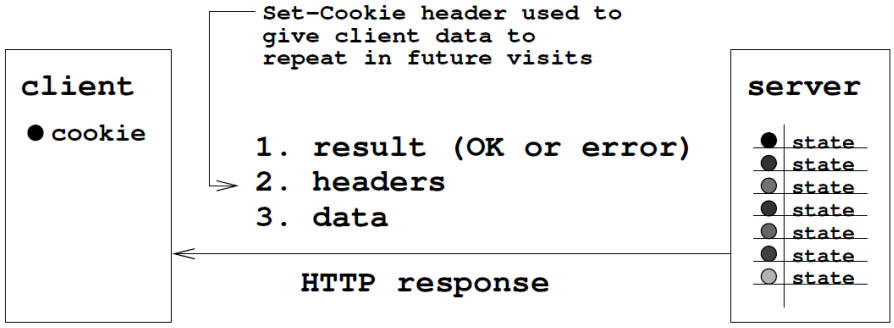
[12] *Company*, SHARETHROUGH, https://sharethrough.com/company (last visited April 1, 2024).

websites, thereby earning revenue, and allows companies to place advertisements on other companies' websites, thereby driving brand awareness and sales. To achieve this, Sharethrough uses its Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant's Website.

35. The first time a user visits Defendant's 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 Sharethrough Tracker on the user's browser. The Sharethrough Tracker, in turn, instructs the user's browser to send Sharethrough the user's IP address.

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

Figure 2:



37. If the user clears his or her cookies, then the user wipes out the Sharethrough

Tracker from its cache. Accordingly, the next time the user visits Defendant's Website the process begins over again: (i) Defendant's server installs the Sharethrough Tracker on the user's browser, (ii) the Sharethrough Tracker instructs the browser to send Sharethrough the user's IP address, (iii) the Sharethrough Tracker stores a cookie in the browser cache, and (iv) Sharethrough will continue to receive the user's IP address on subsequent Website visits with the cookie transmission.

38. In all cases, however, Sharethrough receives a user's IP address each and every time a user interacts with the website of one of Sharethrough's clients, including Defendant's Website. Indeed, the IP address is transmitted to Sharethrough along with the cookie value, as the below screenshot indicates. *See* Figure 3.

//

//

//

//

//

//

//

//

//

//

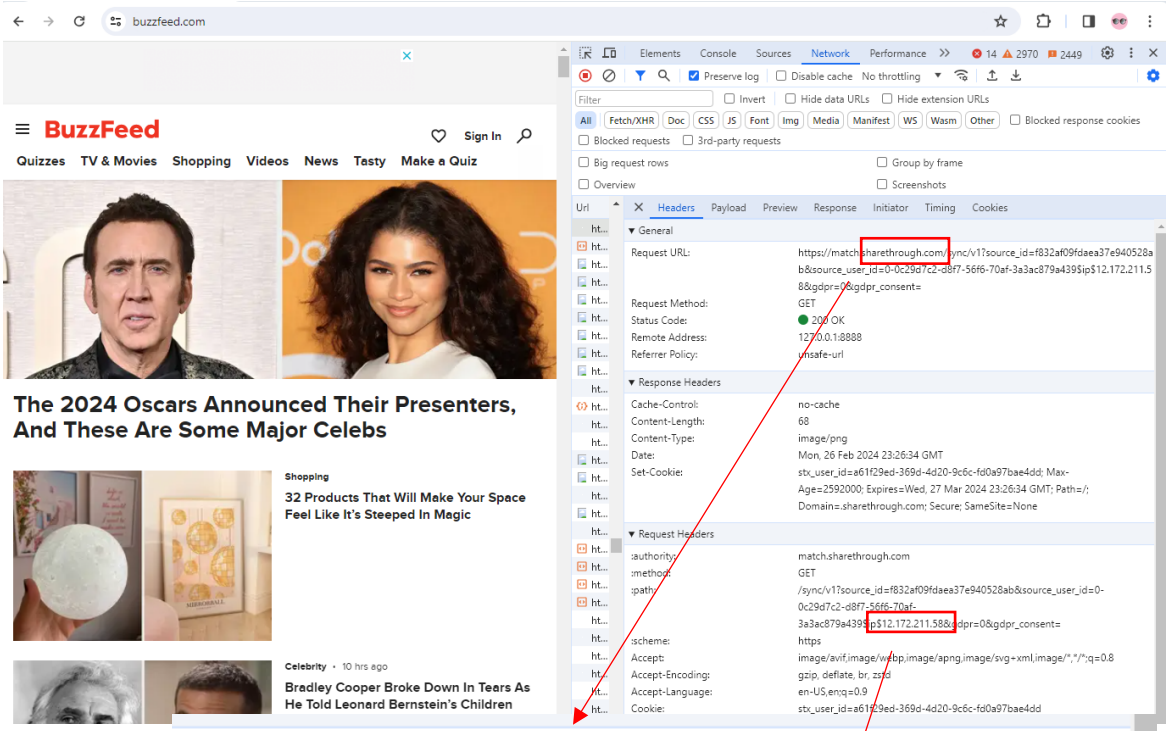
//

//

//

//

Figure 3:



https://match.sharethrough.com/sync/v1?source_id=f832af09fdaea37e940528ab&source_user_id=0-0c29d7c2-d8f7-56f6-70af-3a3ac879a439ip12.172.211.58&gdpr=0&gdpr_consent=
GET
200 OK
127.0.0.1:8888
unsafe-url

no-cache
68
image/png
Mon, 26 Feb 2024 23:26:34 GMT
stx_user_id=a61f29ed-369d-4d20-9c6c-fd0a97bae4dd; Max-Age=2592000; Expires=Wed, 27 Mar 2024 23:26:34 GMT; Path=/; Domain=.sharethrough.com; Secure; SameSite=None

match.sharethrough.com
GET
/sync/v1?source_id=f832af09fdaea37e940528ab&source_user_id=0-0c29d7c2-d8f7-56f6-70af-3a3ac879a439ip12.172.211.58&gdpr=0&gdpr_consent=

39. The Sharethrough 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.

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

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

2. IQM Tracker

42. IQM Corporation ("IQM") is an "industry-specific programmatic media buying and audience intelligence platform."[13]

43. According to IQM, it "employs advanced targeting technologies to reach your desired audience accurately, based on demographic, location, interests, and content consumption."[14]

44. IQM uses its tracking technology to receive, store, and analyze information collected from website visitors, such as visitors of Defendant's Website. IQM uses this data to provide information to its customers on its users' characteristics, including their location, content consumption, browser and devices used, and other information that is highly desirable to customers, allowing them to target customers with precision for advertising and other purposes.

45. The first time a user visits Defendant's Website, the user's browser sends an HTTP request to Defendant's server, and Defendant's server sends an HTTP response with directions to

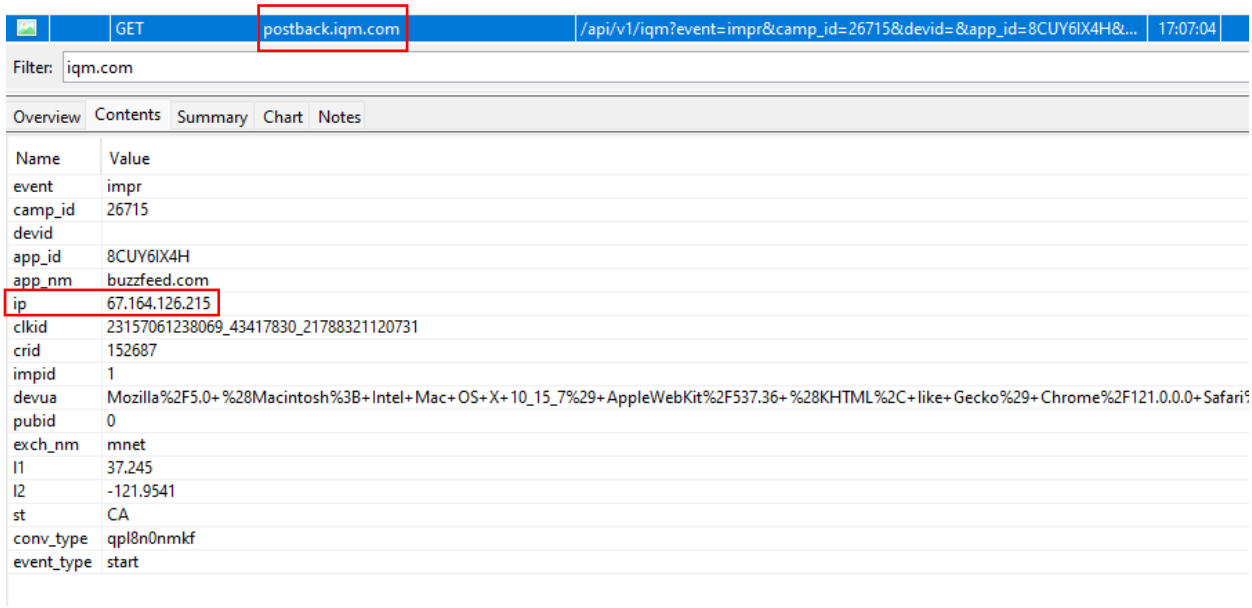
[13] *About Us*, IQM, https://iqm.com/company/about-us (last visited Feb. 28, 2024).

[14] *Self-Serve Platform*, IQM, https://iqm.com/platform/self-serve-platform (last visited April 1, 2024).

install the IQM Tracker on the user's browser. The IQM Tracker, in turn, instructs the user's browser to send IQM the user's IP address.

46. In all cases, however, IQM receives a user's IP address each and every time a user interacts with the website of one of IQM's clients, including Defendant's Website. Indeed, the IP address is transmitted to IQM, as the below screenshot indicates. *See* Figure 4.

Figure 4:



47. The IQM 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.

48. Further, the IQM Tracker is a "device" because "in order for software to work, it must be run on some kind of computing device." *James*, 2023 WL 7392285, at *13.

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

3. Dotomi Tracker

50. Epsilon Data Management, LLC, ("Epsilon") is a software-as-a-service company

that develops the Dotomi Tracker, which it provides to website owners like Defendant for a fee.

51. According to Epsilon, it "reaches across channels to people who are hidden from other partners—including valuable Apple device users and your offline customers," and is "the only digital partner that connects every digital impression to a real person. Everything is optimized to deliver real business outcomes, no matter your objectives."[15]

52. In other words, Epsilon 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, Epsilon uses its Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant's Website.

53. The first time a user visits Defendant's 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 Dotomi Tracker on the user's browser. The Dotomi Tracker, in turn, instructs the user's browser to send Epsilon the user's IP address.

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

[15] *Epsilon Digital*, EPSILON, https://www.epsilon.com/us/products-and-services/epsilon-digital, (last visited April 1, 2024).

55. If the user clears his or her cookies, then the user wipes out the Dotomi Tracker from its cache. Accordingly, the next time the user visits Defendant's Website the process begins over again: (i) Defendant's server installs the Dotomi Tracker on the user's browser, (ii) the Dotomi Tracker instructs the browser to send Epsilon the user's IP address, (iii) the Dotomi Tracker stores a cookie in the browser cache, and (iv) Epsilon will continue to receive the user's IP address on subsequent Website visits with the cookie transmission.

56. In all cases, however, Epsilon receives a user's IP address each and every time a user interacts with the website of one of Epsilon's clients, including Defendant's Website. Indeed, the IP address is transmitted to Epsilon along with the cookie value, as the below screenshot indicates. *See* Figure 5.

//

//

//

//

//

//

//

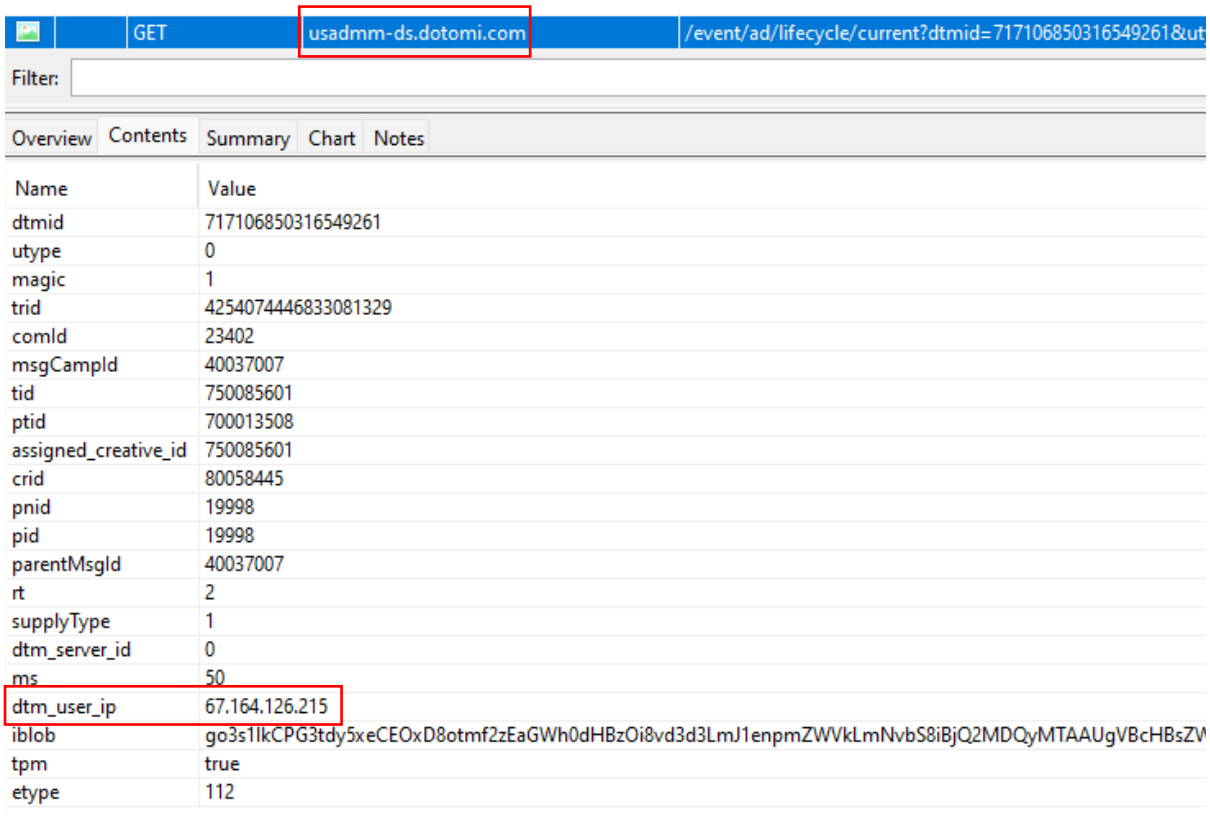
//

//

//

//

Figure 5:



57. The Dotomi 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.

58. Further, the Dotomi Tracker is a "device" because "in order for software to work, it must be run on some kind of computing device." *James*, 2023 WL 7392285, at *13.

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

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

60. Defendant owns and operates the Website. According to Defendant, "BuzzFeed, Inc. is home to the best of the Internet. Across food, news, pop culture and commerce, our brands drive conversation and inspire what audiences watch, read, buy, and obsess over next. Born on the Internet in 2006, BuzzFeed, Inc. is committed to making it better: providing trusted, quality,

brand-safe news and entertainment to hundreds of millions of people; making content on the Internet more inclusive, empathetic, and creative; and inspiring our audience to live better lives."[16]

61. 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.[17]

62. Often times, third-party scripts are installed on websites "for advertising purposes."[18]

63. 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."[19]

64. Since at least June 2019, if not earlier, Defendant has incorporated the code of these Trackers into the code of its Website. Thus, when Plaintiff visited the Website, the Website caused the Trackers to be installed on Plaintiff's and other users' browsers.

65. 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.

66. Upon installing the Trackers on its Website, the Trackers collect the IP address of visitors to the Website, including the IP address of Plaintiff and Class Members. *See* Figures 3-5, *supra*.

67. The operators of the Trackers then use the IP address of Website visitors, including those of Plaintiff and Class Members, to serve targeted advertisements and conduct website

---

[16] *About*, BUZZFEED, https://www.buzzfeed.com/about (last visited April 1, 2024).

[17] *See Third-party Tracking*, PIWIK, https://piwik.pro/glossary/third-party-tracking/ (last visited April 1, 2024) ("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…").

[18] *Id*.

[19] *Id*.

analytics.

68. 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.

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

69. 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.

70. 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 Sharethrough Tracker For The Purposes of Marketing, Advertising, And Analytics

71. Sharethrough is an AdTech platform that prides itself on "Enhancing the Ad Experience[,] Across Every Channel[,] For Better Outcomes."[20] Sharethrough "maximizes user attention & performance through research-backed ad enhancements while curating the inventory for optimized directness, sustainability and quality."[21]

72. Sharethrough helps companies like Defendant market, advertise, and analyze user data from its website. One way Sharethrough assists with marketing is through its Audiences Curation Packages, which allow its clients to place their ads on curated sites, with intentional

[20] SHARETHROUGH, https://sharethrough.com/ (last visited April 1, 2024).

[21] *Id.*

placement, and targeted at specific audiences "based on data, demographic[s,] and site content to reach advertiser audiences at scale."[22] For example, Sharethrough will help advertisers target Super Bowl fans, members and allies of the LGBTQ community, and individuals in the Gen Z population.[23]

73. Sharethrough also helps clients place ads on their website, thereby ensuring "publishers yield the strongest performance of their ad inventory."[24] By optimizing who sees what ads on a client's website, "Sharethrough's technology help[s] hundreds of publishers drive more revenue and generate better ad performance."[25]

74. In order to perform the functions listed above, Sharethrough needs to collect data that identifies a particular user. This is why Sharethrough collects IP addresses: it allows Sharethrough to ascertain a user's identity and target that user with personalized advertisements, 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.

75. In other words, when users visit Defendant's Website, Sharethrough collects users' IP addresses through its Sharethrough 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 allowing third parties to collect user information.

---

[22] *Advertisers*, SHARETHROUGH, https://sharethrough.com/advertisers/curation (last visited April 1, 2024).

[23] *Id.*

[24] *Publishers*, SHARETHROUGH, https://sharethrough.com/publishers (last visited April 1, 2024).

[25] *Id.*

2. Defendant Uses The IQM Tracker For The Purposes of Marketing, Advertising, And Analytics

76. IQM is a media buying and audience intelligence platform that claims, "Our technology is one of the best in the world for data security, audience intelligence, location intelligence, AI, contextual intelligence, and optimization."[26] IQM provides a Demand-Side Platform ("DSP"), which is a type of software that allows an advertiser to buy advertising with the help of automation.

77. IQM bills its product as an "industry-specific advertising technology platform"[27] providing audience, location, and contextual targeting for political, healthcare, B2B, finance, travel, retail, and "sensitive" (i.e. cannabis) industries. This means that IQM assists customers with their advertising campaigns in:

- Audience targeting ("Segment audience & reach people based on identity, interests, location, and past ad interactions");
- Location targeting ("Use location based targeting technologies such as geofencing and geofarming to reach consumers with high precision")
- Contextual targeting ("Use IQM's proprietary AI technology to target users by the content consumption behavior")
- Creative AI ("Creative AI technology abstracts contextual data from ad creatives and matches it with curated ad inventory and audiences.")[28]

78. In order to perform the functions listed above, IQM needs to collect data that

[26] *Our Technologies*, IQM, https://iqm.com/platform/our-technologies (last visited April 1, 2024).

[27] IQM, https://iqm.com/ (last visited April 1, 2024).

[28] *Target users by location*, IQM, https://iqm.com/retail (last visited April 1, 2024).

identifies a particular user. This is why the IQM Tracker collects IP addresses: it allows IQM to ascertain a user's identity and target that user with personalized advertisements, 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.

79. In other words, when users visit Defendant's Website, IQM through its IQM Tracker collects users' IP addresses 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 allowing third parties to collect user information.

3. Defendant Uses The Dotomi Tracker For The Purposes of Marketing, Advertising, And Analytics

80. Epsilon is a global advertising and marketing technology company and "is the only digital advertising services partner that connects every display, online video, connected TV and audio impression to a real person."[29]

81. Epsilon helps companies like Defendant market, advertise, and analyze user data from its website. For example, Epsilon recognizes that its clients want "[t]o move potential customers from awareness to action" and thus "need to know who [the clients are] reaching."[30] Thus, with Epsilon's "COREID, the industry's only identity solution using all available online and offline identifiers, brands can reach the right person across their favorite content on any device."[31]

82. Indeed, Epsilon boasts that it has "[u]nrivaled accuracy at an individual level"

[29] *Epsilon Digital*, EPSILON, https://www.epsilon.com/us/products-and-services/epsilon-digital (last visited April 1, 2024).

[30] *Epsilon Digital | Online Video*, EPSILON, https://www.epsilon.com/us/products-and-services/epsilon-digital/online-video (last visited April 1, 2024).

[31] *Id.*

because its technology requires a "complete name and address validated by transactions" to "ensure[e] marketers reach the right person with maximum precision and efficiency."[32] "The COREID graph of 200M+ U.S. consumers is the only solution grounded in offline names and address, enabling omnichannel people-based activation, measurement and waste reduction."[33]

83. In order to perform the functions listed above, Epsilon needs to collect data that identifies a particular user. This is why the Dotomi Tracker collects IP addresses: it allows Epsilon to ascertain a user's identity and target that user with personalized advertisements, 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 Website, Epsilon through its Dotomi Tracker collects users' IP addresses 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 allowing third parties to collect user information.

III. PLAINTIFF'S EXPERIENCE

85. Plaintiff has visited the Website multiple times—including as long ago as June 2019 and as recently as March 2024—on her desktop browser.

86. When Plaintiff visited the Website, the Website's code—as programmed by Defendant—caused the Trackers to be installed on Plaintiff's browser. Defendant, Sharethrough, IQM, and Epsilon then used the Trackers to collect Plaintiff's IP address. *See* Figures 6 (Sharethrough Tracker), 7 (IQM Tracker), and 8 (Dotomi Tracker).

---

[32] *Identity: COREID*, EPSILON, https://www.epsilon.com/us/products-and-services/identity-core-id (last visited April 1, 2024).

[33] *Id.*

Figure 6:

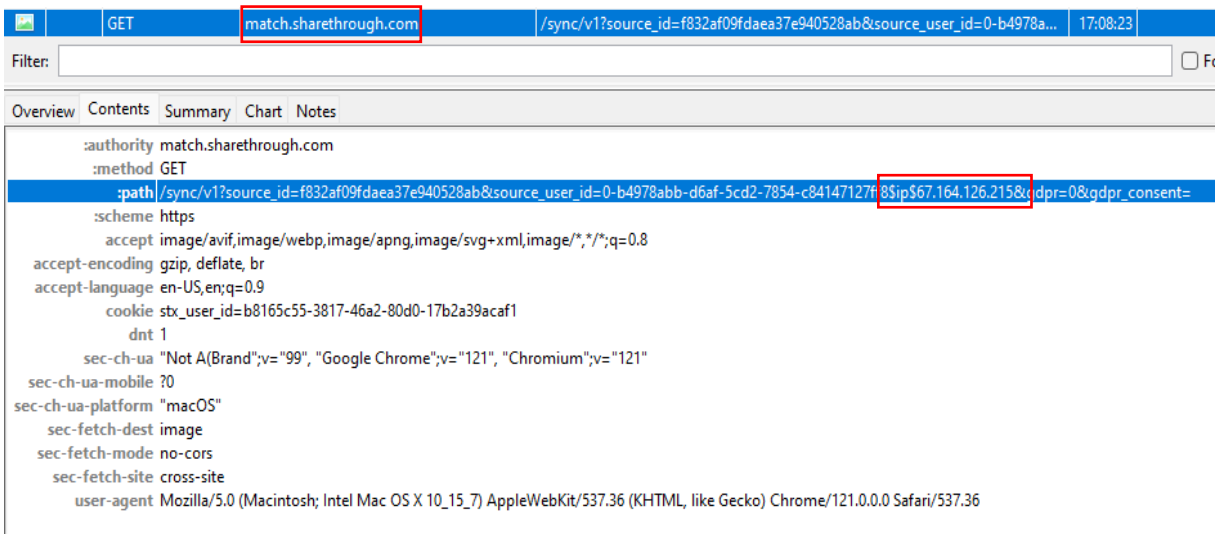


Figure 7:

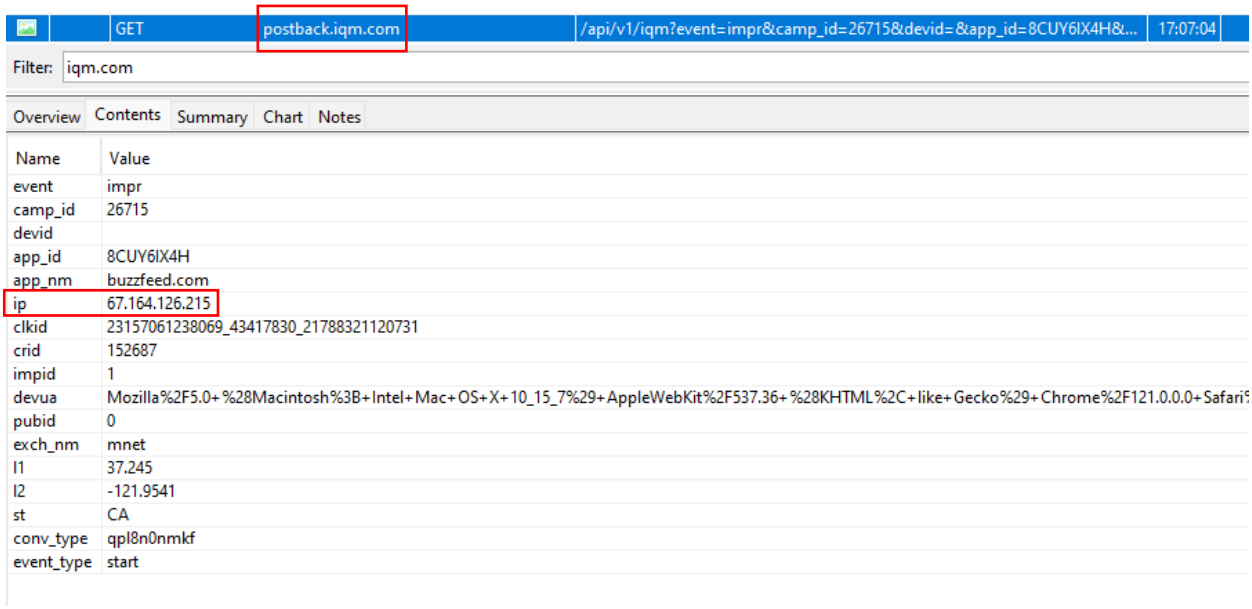
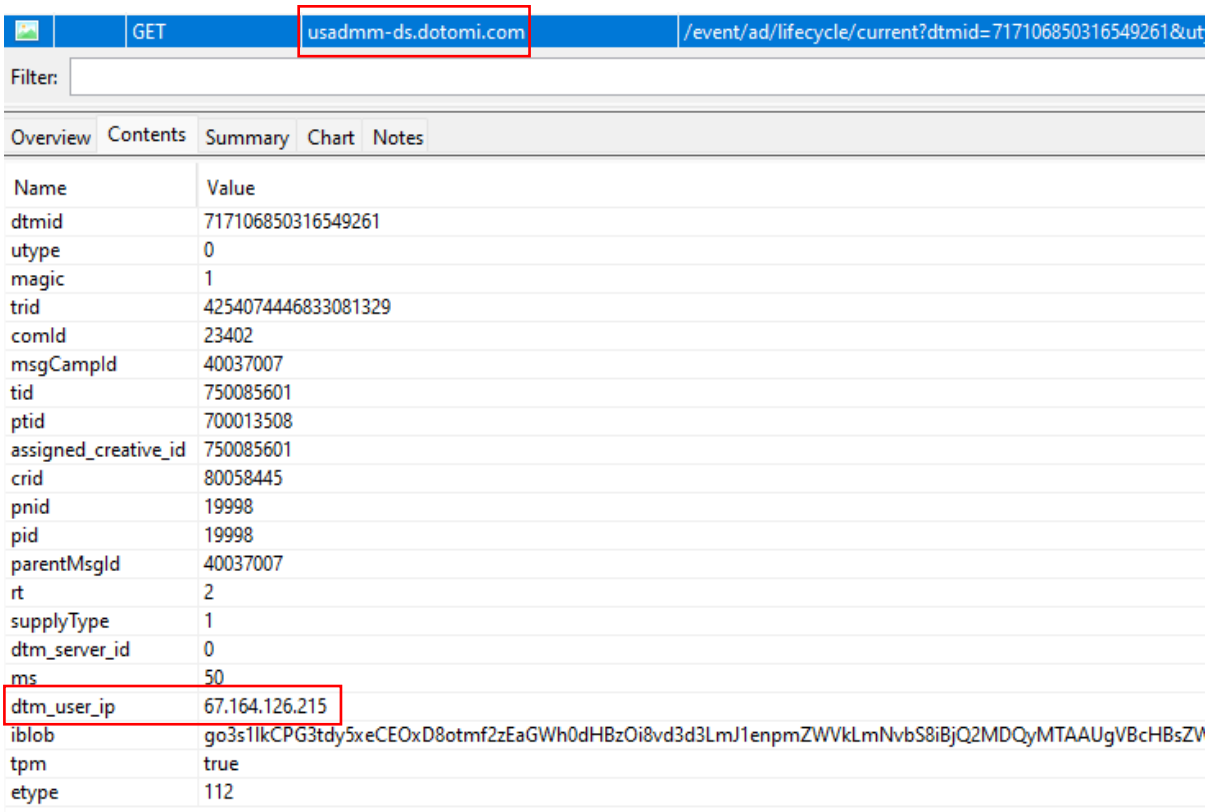


Figure 8:



87. Defendant, Sharethrough, IQM, and Epsilon used the information collected by the Trackers to analyze Website data and marketing campaigns, conduct targeted advertising, and ultimately boost Defendant's and advertisers' revenue.

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

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

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

CLASS ALLEGATIONS

91. Pursuant to Fed. R. Civ. P. 23(a) and 23(b)(3), Plaintiff seeks to represent a class defined as all California residents who accessed the Website in California and had their IP address collected by any of the Trackers (the "Class").

92. 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.

93. **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.

94. **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 § 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.

95. **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 Website and had her IP address collected by the Trackers, which were installed and used by Defendant.

96. **Adequate Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class Members she seeks to represent, she has retained competent counsel experienced in prosecuting class actions, and she intends to prosecute this action vigorously. The interests of members of the Class will be fairly and adequately protected by Plaintiff and her counsel.

97. **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)

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

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

100. CIPA § 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."

101. 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).

102. The Trackers are "pen registers" because they are each a "device or process" 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).

103. At all relevant times, Defendant installed each Tracker—which is a pen register—on Plaintiff's and Class Members' browsers, and used the Trackers to collect Plaintiff's and Class Members' IP addresses.

104. The Trackers do not collect the content of Plaintiff's and the Class's electronic communications with the Website. *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).

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

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

107. 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.

DEMAND FOR JURY TRIAL

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

Dated: April 11, 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