

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

1 ERIC A. GROVER (SBN 136080)
2 [eagrover@kellergrover.com](mailto: eagrover@kellergrover.com)
3 RACHAEL G. JUNG (SBN 239323)
4 [rjung@kellergrover.com](mailto: rjung@kellergrover.com)
5 **KELLER GROVER LLP**
6 1965 Market Street
7 San Francisco, California 94103
8 Telephone: (415) 543-1305
9 Facsimile: (415) 543-7861

6 SCOT BERNSTEIN (SBN 94915)
7 [swampadero@sbernsteinlaw.com](mailto: swampadero@sbernsteinlaw.com)
8 **LAW OFFICES OF SCOT D. BERNSTEIN,**
9 **A PROFESSIONAL CORPORATION**
10 101 Parkshore Drive, Suite 100
11 Folsom, California 95630
12 Telephone: (916) 447-0100
13 Facsimile: (916) 933-5533

Attorneys for Plaintiffs
Ryan Wu and Saber Khamooshi

ELECTRONICALLY
FILED

*Superior Court of California,
County of San Francisco*

07/23/2024
Clerk of the Court

BY: ANNIE PASCUAL
Deputy Clerk

SUPERIOR COURT OF THE STATE OF CALIFORNIA
IN AND FOR THE COUNTY OF SAN FRANCISCO

16 RYAN WU and SABER KHAMOOSHI,
17 individually and on behalf of a class of
18 similarly situated individuals,
19
20 Plaintiffs,

v.

20 GANNETT CO., INC.; and DOES 1 through
21 100, inclusive,
22
23 Defendants.

) Case No: CGC-24-615921

) CLASS ACTION

) **FIRST AMENDED COMPLAINT FOR DAMAGES**

) **DEMAND FOR JURY TRIAL**

) Action Filed: June 26, 2024

1 **CLASS ACTION COMPLAINT**

2 Plaintiffs Ryan Wu and Saber Khamooshi, on behalf of themselves and a class of similarly
3 situated individuals as defined below, and based on personal knowledge where applicable,
4 information and belief, and investigation by counsel, alleges the following against Defendant
5 Gannett Co., Inc.

6 **INTRODUCTION**

7 1. This class action lawsuit arises out of Defendant’s policy and practice of embedding
8 and using various trackers on Defendant’s USA Today website, www.usatoday.com, to (1) install
9 and store third-party tracker cookies on website users’ browsers and (2) collect website users’
10 personally identifying and addressing information, such as IP addresses¹, that the USA Today
11 website surreptitiously discloses and shares with the third-party trackers without users’ knowledge,
12 authorization, or consent.

13 2. Defendant Gannett Co., Inc. (“Defendant” or “Gannett”) is an American mass
14 media holding company that owns and publishes various brands that deliver journalism,
15 compelling content, events, experiences, and digital marketing business solutions. Gannett’s
16 portfolio includes hundreds of brands and local media outlets across the United States and United
17 Kingdom, including USA Today, The Arizona Republic, Golfweek, Newsquest Media Group, and
18 many others.

19 3. Founded in 1980 and launched in 1982, USA Today is a newspaper and news
20 broadcasting company that operates from Gannett’s corporate headquarters in New York. USA
21 Today covers breaking news, politics, sports, entertainment, money, wellness and more. Its
22 newspaper is printed at 37 sites across the United States and at five additional sites internationally.
23 Defendant also owns and operates the www.usatoday.com website (the “USA Today website”),
24 which provides breaking news and in-depth coverage of U.S. and national news.

25
26
27 ¹ IP addresses have been classified by the United States Department of Health and Human Services (“HHS”) as personally identifying information. *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Department of Health and Human Services (Dec. 1, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>
28

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

1 9. While physically present in California, Plaintiff Wu regularly has visited and still
2 visits the USA Today website to browse news headlines and read articles. He visited the USA
3 Today website as recently as May 2024. Plaintiff Wu used and continues to use an internet browser
4 on his computer and on his cellular phone to access Defendant’s website.

5 10. While physically present in California, Plaintiff Khamooshi regularly has visited
6 and still visits the USA Today website to browse news headlines and read articles. He visited the
7 USA Today website as recently as June 2024. Plaintiff Khamooshi used and continues to use an
8 internet browser on his computer and on his cellular phone to access Defendant’s website.

9 11. At no time when either Plaintiff entered the USA Today website and viewed its
10 content did either Plaintiff authorize Defendant to install or consent to Defendant installing third-
11 party tracker cookies on his internet browser or computer.

12 12. Plaintiffs also did not consent to Defendant sharing and selling their IP addresses
13 and other personally identifying information with or to third-party trackers. Further, because
14 Defendant did not provide notice or request permission, Plaintiffs were unaware of and had no
15 opportunity to opt out of that unauthorized disclosure of his data.

16 **B. Defendant Gannett Co., Inc., and the USA Today Website**

17 13. Defendant Gannett Co., Inc. is a corporation organized under the laws of the State
18 of Delaware with its headquarters and principal place of business in New York, New York.
19 Defendant systematically and continuously does business in California and with California
20 residents.

21 14. Defendant currently owns and operates the www.usatoday.com website, which
22 publishes breaking news, politics, sports, entertainment, money, wellness and more from across
23 the country and around the world.

24 15. Defendant’s USA Today website fails to put visitors on notice of Defendant’s use
25 of website tracking technology, including its use of third-party trackers. Upon information and
26 belief, Plaintiffs allege that third-party trackers allow and enable companies like and including
27 Defendant to sell advertising space on their websites by using the tracking technology to receive,
28 store, and analyze information collected from website visitors.

1 claims occurred in the State of California, including Plaintiffs' accessing of and interactions with
2 the USA Today website, Defendant's installing of third-party tracker cookies on California users'
3 web browsers, and Defendant's collecting and unauthorized sharing of Plaintiffs' and Class
4 members' personally identifying and addressing information. Plaintiffs' rights were violated in
5 the State of California and those violations arose out of his contact with Defendant from and within
6 California.

7 21. Venue is proper in this Court because Code of Civil Procedure §§ 395 and 395.5
8 and case law interpreting those sections provide that if a foreign business entity fails to designate
9 with the office of the California Secretary of State a principal place of business in California, it is
10 subject to being sued in any county that a plaintiff desires. On information and belief, Defendant
11 Gannett Co., Inc. is a foreign business entity and had failed to designate a principal place of
12 business in California with the office of the Secretary of State as of the date this Complaint was
13 filed.

14 **FACTUAL ALLEGATIONS COMMON TO THE CLASS**

15 **A. Website Tracking Technology**

16 22. Trackers are companies that collect information about internet users as those users
17 browse the web. Trackers use cookies, scripts or pixels inserted by publishers or advertisers.
18 Tracker profiling is the process of linking data from different sites to build profiles of individual
19 internet users based on their browsing history, to place those internet users in groups, and to sell
20 those persons' profiles and that data to third parties for targeted advertising.

21 23. There is a broad range of online technologies that track and monitor internet-based
22 interactions and communications. Four identifier tools commonly used are (i) website cookies,
23 (ii) tracking pixels, (iii) digital fingerprinting, and (iv) software development kits.

24 24. A website cookie refers to a small text file that a website server creates and
25 transmits to a web browser (*e.g.*, Google Chrome or Safari). The receiving web browser then
26 installs and stores the file in a particular directory on an individual's computer, phone, or other
27
28

1 device.² Essentially, when a website user attempts to access a webpage, the user’s browser
2 transmits a communication to the website’s server requesting that the server display the website’s
3 content for the browser to load. While providing the requested content to the user, the website’s
4 server also provides the cookies that it would like the user’s browser to install and retain.

5 25. Website cookies contain information that identifies the domain name of the
6 webserver that wrote the cookie (e.g., www.hulu.com or www.facebook.com). Cookies also have
7 information about the user’s interaction with a website, such as how the website should be
8 displayed, how many times a user has visited the website, what pages the user visited, and
9 authentication information. In addition to a unique identifier and a site name, website cookies also
10 can include personally identifiable information such as a user’s name, address, email address or
11 phone number if that information was provided to a website.

12 26. A first-party cookie is implemented by the website the user accesses. The website
13 uses its cookies for authentication, monitoring user sessions, and collecting analytical data. A
14 third-party cookie, also called an “advertising cookie” or “tracker cookie,” is a cookie that belongs
15 to a domain other than the one being displayed to the user in the user’s browser. The key
16 differences between the first-party and third-party cookies are who sets them (*i.e.*, a website
17 display host or a third party), whether and how they can be blocked by a web browser, and the
18 availability of the cookie. A third-party advertising or tracker cookie is available and accessible
19 on *any* website that loads the third-party server’s code, not just on the host website that the user is
20 trying to access. Third-party cookies typically are used for cross-site tracking, retargeting, and ad-
21 serving.

22 27. A pixel, also known as a “tracking pixel,” “web bug,” “clear GIF” or “web beacon,”
23 is similar to a website cookie. It is a small, almost invisible image (pixel) embedded in a website
24 or an email to track a user’s activities. This data often includes the user’s operating system, the
25 type of website or email used, the time at which the website was accessed, the user’s IP address,
26

27
28 ² See Sara J. Nguyen, *What Are Internet Cookies and How Are They Used? All About Cookies*
(Jul. 28, 2023), <https://allaboutcookies.org/what-is-a-cookie>.

1 and whether there are cookies that previously have been set by the server hosting the pixel image.³

2 28. “Digital fingerprinting” refers to device fingerprinting and browser fingerprinting,
3 both of which send information to the website server to help ensure that a website is displaying
4 content and operating in accordance with its specifications. Although a browser or device does
5 not usually transmit personal information about a user, most fingerprinting is performed via a third-
6 party tracker, which can track an individual across multiple sites and form a profile of the user.⁴

7 29. A software development kit (SDK) is a set of computer programs and similar tools
8 that developers and engineers can leverage to build applications for specific platforms. The SDK
9 often includes, among other tools, libraries, application programming interfaces, instructions,
10 guides, directions, and tutorials.⁵ SDKs also may have embedded code that allows them to
11 intercept personal data and other information from application users surreptitiously. That data and
12 information can include geolocation data, usernames and communications derived from other SDK
13 applications installed on a user’s device, and a user’s activities within an application after
14 installation.

15 30. All of the information and data captured and collected by third-party trackers,
16 regardless of the tool used, is capable of being sold and used for marketing and advertising
17 purposes.

18 **B. Internet Protocol Addresses (“IP Addresses”)**

19 31. One important piece of identifying information collected by third-party trackers is
20 a website user’s IP address. An IP address is a unique identifier for a device and is written as four
21 sets of numerals separated by decimal points (e.g., 123.145.167.189). The first two sets of
22 numerals identify the device’s network. The second two sets of numerals identify the specific
23 device itself. The IP address enables a device to communicate with another device, such as a
24 _____

25 ³ See Patti Croft & Catherine McNally, *What Is a Web Beacon and Why Should You Care? All*
26 *About Cookies* (Sept. 26, 2023), <https://allaboutcookies.org/what-is-a-web-beacon>.

27 ⁴ See Anokhy Desai, *The Half-Baked Future of Cookies and Other Tracking Technologies*, IAPP
(July 2023), <https://iapp.org/resources/article/future-of-cookies-tracking-technologies/>.

28 ⁵ *What Is an SDK? Software Development Kits Explained*, Okta, Inc. (June 30, 2022),
<https://www.okta.com/identify-101/what-is-an-sdk>.

1 computer's web browser communicating with a website's server.

2 32. Similar to a telephone number for a person, an IP address is a unique numerical
3 code associated with a specific internet-connected device on a computer network. The IP
4 addresses identify all of the devices accessing a certain network at any given time.

5 33. Importantly from a privacy perspective, an IP address contains geographical
6 location information from which the state, city and zip code of a specific device can be determined.
7 Given the information that it can and does reveal, an IP address is considered personally
8 identifiable information and is subject to HIPAA protection.⁶

9 34. Being able to know a website user's IP address, and therefore the user's geographic
10 location, provides "a level of specificity previously unfound in marketing."⁷ An IP address allows
11 advertisers to target customers by countries, cities, neighborhoods, and postal codes.⁸ Even more
12 specifically, it allows advertisers to target specific households, businesses, and even individuals
13 with ads that are relevant to their interests.⁹

14 35. Indeed, because it enables companies to use an IP address to identify individuals
15 personally, IP targeting is one of the most successful marketing techniques that companies can
16 employ to spread the word about a product or service.¹⁰ By targeting specific households or
17 businesses, a company can avoid wasting money on ads that are unlikely to be seen by their target
18 audience and instead can reach their target audience with far greater precision.¹¹ Additionally, by
19
20

21 ⁶ See 45 C.F.R. § 164.514(b)(2)(i)(O).

22 ⁷ *IP Targeting: Understanding This Essential Marketing Tool*, AccuData,
<https://www.accudata.com/blog/ip-targeting/> (last visited June 17, 2024).

23 ⁸ *Location-based Targeting That Puts You in Control*, Choozle,
<https://choozle.com/geotargeting-strategies/> (last visited June 17, 2024).

24 ⁹ Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LinkedIn (Nov.
25 29, 2023), <https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf/>

26 ¹⁰ Trey Titone, *The future of IP address as an advertising identifier*, Ad Tech Explained (May 16,
27 2022), <https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/>

28 ¹¹ 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/>

1 analyzing data regarding which households or businesses are responding to their ads, IP address
2 targeting can help businesses improve their overall marketing strategies and refine their marketing
3 efforts.¹²

4 36. As alleged below, Defendant installed and continues to install third-party tracker
5 cookies on USA Today website users' browsers. Those trackers have collected and continue to
6 collect identifying and addressing information about Plaintiffs and Class members, including their
7 IP addresses, without a court order and without those individuals' consent.

8 **C. Defendant's Use of Third-Party Trackers on the USA Today Website**

9 37. Defendant has embedded and implemented several third-party trackers on the USA
10 Today website, including but not limited to (i) Taboola Tracker, (ii) Amobee Tracker and (iii)
11 Adnx Tracker (the "trackers"). By installing these trackers and their corresponding tracking
12 cookies, Defendant can sell advertising space on the USA Today website. That enables Defendant
13 to monetize its website further and to maximize its revenue by collecting and disclosing user
14 information.

15 38. Taboola Tracker is developed by software company Taboola Inc., which leverages
16 data analytics to align digital content with user preferences across its network of publisher
17 websites. As a content recommendation platform, the Taboola Tracker is designed to collect user
18 data to optimize content suggestions, enhancing both user experience and content monetization for
19 publishers.

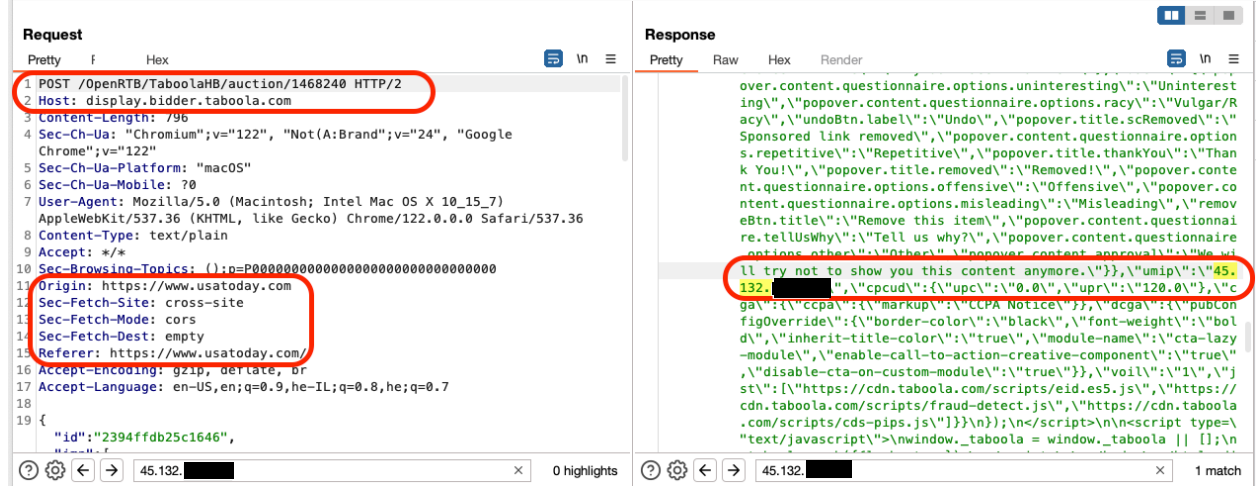
20 39. When a website user first accesses and enters the USA Today website, the user's
21 browser sends an HTTP request¹³ to Defendant's website server. Defendant's website server sends
22 an HTTP response with directions to load the webpage content and to install the Taboola Tracker
23 on the user's browser. The Taboola Tracker stores a website cookie in the user's browser cache
24 and uses that third-party tracker cookie to collect and share that user's IP address with Taboola
25

26 _____
27 ¹² *Id.*

28 ¹³ HTTP stands for "HyperText Transfer Protocol." It is the computer communication protocol used for most communication on the world wide web.

every time the user interacts with the USA Today website. See Figure 1, identifying Taboola, www.usatoday.com, and the user’s IP address (45.132.xxx.xxx).

Figure 1:



KELLER GROVER LLP
 1965 Market Street, San Francisco, CA 94103
 Tel. 415.543.1305 | Fax 415.543.7861

40. This entire process takes place behind the scenes in less than a second. Thus, the Taboola Tracker cookie appears the moment the user enters the USA Today website, and it is installed without any further action or consent required of the user.

41. Further, each time a user revisits the USA Today website, the Taboola Tracker identifies that user and sends the stored website cookie, including the user’s IP address, back to Taboola. *Even if a user clears the cookies from the user’s browser, it makes no difference:* the next time that user visits the USA Today website, the Taboola Tracker re-installs the tracker cookie, resets the tracking process, and resumes transmission of the user’s IP address to Taboola on future visits.

42. Taboola collects IP addresses to allow it to ascertain a user’s location and target that user with advertisements tailored to that specific location. According to its website, Taboola uses its “unique data about people’s interests and information consumption to recommend the right content to the right person at the right time.”¹⁴ Taboola assists advertisers with targeting their

¹⁴ *How Taboola Works*, Taboola Help Center, <https://help.taboola.com/hc/en-us/articles/115006597307-How-Taboola-Works> (last visited June 17, 2024).

1 campaigns by location, time, browser type, connection type, audience segments, and more.¹⁵

2 43. In addition to the Taboola Tracker, Defendant also embeds the Amobee Tracker on
3 its USA Today website. Like the Taboola Tracker, the Amobee Tracker is installed the moment a
4 user accesses the USA Today website, all without any notice to or request for permission from the
5 user.

6 44. Amobee is a digital marketing technology company that delivers a broad spectrum
7 of advertising solutions aimed at helping brands, agencies, and publishers navigate the digital
8 landscape. With an ad-serving platform that integrates across various channels such as digital,
9 social, mobile, and video, Amobee delivers targeted advertising content to users based on their
10 browsing habits and other collected data, including their IP addresses. Amobee utilizes HTTP
11 requests and responses, along with cookies and IP addresses, to track and deliver personalized ads
12 to users on host sites like USA Today.

13 45. Specifically, when a user visits the USA Today website, an HTTP request is sent
14 to Amobee's servers, which includes the user's IP address and allows Amobee to identify the
15 user's geographic location. Amobee's servers then leverage the information contained within the
16 user's HTTP request to respond with targeted ads tailored to the user.

17 46. Amobee installs third-party tracker cookies on the user's browser during this
18 process. Those cookies, which also store information linked to the user's browsing behavior,
19 enable Amobee to recognize the user on subsequent visits to USA Today or to other websites
20 within Amobee's advertising network and thereby leverage the user's personal browsing
21 preferences. *See* Figure 2, identifying Amobee, www.usatoday.com, and the user's IP address
22 (45.132.xxx.xxx).¹⁶

23 **Figure 2:**

24

25

26 ¹⁵ *Id.*

27 ¹⁶ The host name "presentation-pdx1.turn.com" signifies the presence of the Amobee tracker.
28 Amobee is the name of the advertising platform, but its tracking cookies use the "[turn.com](https://www.turn.com)"
domain. *See* <https://www.netify.ai/resources/domains/turn.com>.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

The screenshot displays the network developer tools for a request to `presentation-pdx1.turn.com`. The request headers include a long cookie string, a user-agent for Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7), and a referer from `https://www.usatoday.com/`. The response is an HTML document containing several JavaScript tracking scripts, including Amobee Tracker and Xandr. A red box highlights the Amobee Tracker script in the response, which includes a `script` tag with a `src` attribute pointing to `https://www.usatoday.com/`.

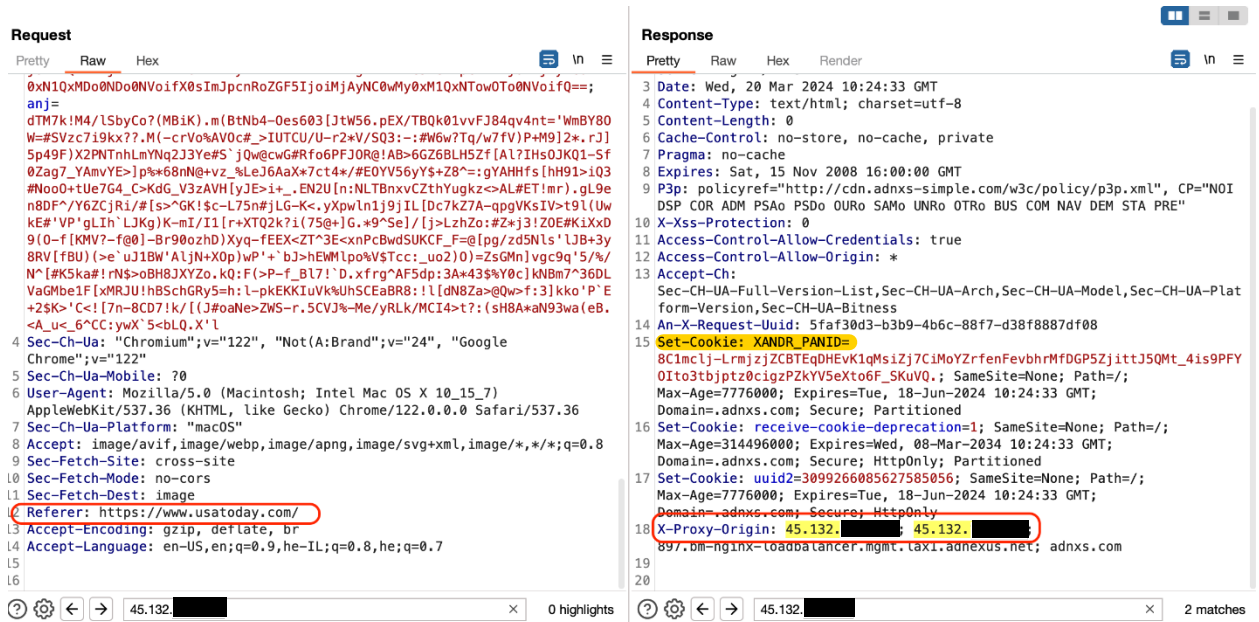
47. *Even if the Amobee Tracker cookies are cleared from the user's browser, the Amobee Tracker is re-installed automatically on subsequent visits to USA Today. The tracking cycle restarts, ensuring that Amobee consistently receives the user's IP address and browsing preferences with every website interaction. This mechanism facilitates a cycle of ad targeting and tracking and increases the relevancy and effectiveness of ads presented by Amobee to users across the web.*

48. The third tracker embedded in Defendant's USA Today website is developed by software company Xandr, which Microsoft acquired in 2021. Xandr operates as an advanced advertising company that claims to provide a comprehensive platform for buying and selling consumer-centric digital advertising. The platform, which includes programmatic advertising, data analytics, and cross-screen media solutions, aims to improve the efficiency and effectiveness of advertising across various channels by leveraging data and technology.

49. Like other third-party trackers, Xandr allows companies like Defendant to sell advertising space on their websites by using the Adnx Tracker to receive, store and analyze information collected from website visitors. The Adnx Tracker is installed and stored on the user's

1 browser the instant the user enters the USA Today website. The third-party tracker cookie then
2 sends the user's IP address to Xandr each and every time the user interacts with the USA Today
3 website. See Figure 3, identifying [Xandr, www.usatoday.com, and the user's IP address
4 (45.132. [REDACTED]).

5 **Figure 3:**



17 50. Each of the three trackers embedded on Defendant's USA Today website (1)
18 installs a third-party tracker cookie on users' browsers and (2) captures, collects, and shares with
19 undisclosed third parties USA Today website users' personally identifying and addressing
20 information, including the users' IP addresses, all without users' knowledge or consent.

21 51. Notably, upon information and belief, the trackers collect IP addresses that can be
22 used to ascertain a user's exact location, potentially with specific latitude-longitude coordinates
23 and a zip code. That information can be used by Defendant and third parties to analyze the USA
24 Today website data and conduct targeted advertising based on a user's location as discussed above.

25 52. Further, each of the three trackers embedded on Defendant's USA Today website
26 *re-installs its tracker cookies every time a user visits the website.* That happens even if the user
27 previously cleared the cookies from his or her web browser cache. As a result, USA Today website
28 users cannot escape the unauthorized sharing of their personally identifying and addressing

1 information with third-parties Taboola, Amobee, and Xandr.

2 **D. Plaintiffs and Class Members Did Not Consent To Defendant’s**
3 **Disclosure of Their Personally Identifying and Addressing Information,**
4 **and They Have a Reasonable Expectation of Privacy in Their User Data.**

5 53. Defendant does not ask its USA Today website visitors, including Plaintiff, whether
6 they consent to having their personally identifying and addressing information disclosed to and
7 used by third parties like Taboola, Amobee, and Xandr. When a website user accesses and enters
8 the USA Today website, there is no pop-up window or other notification to inform users that
9 Defendant is using website tracking technology or installing third-party tracker cookies.

10 54. Additionally, the third-party trackers are incorporated seamlessly – *and, to users,*
11 *invisibly* – in the background on the USA Today website. That seamless and invisible
12 incorporation gave and gives Plaintiffs and Class members no way to know that Defendant was
13 collecting their personally identifying information and IP addresses and secretly sharing them with
14 undisclosed third parties.

15 55. Further, although the USA Today website does have a Privacy Policy containing
16 some disclosures about how information is collected and shared, that policy can be viewed only
17 after scrolling through all of the website content to the very bottom of the webpage. Thus,
18 Defendant’s policies and notices would be seen, if at all, only long after the third-party trackers
19 and cookies had been installed on users’ web browsers.

20 56. In addition to its hard-to-see location, the hyperlink to access the Privacy Policy is
21 written in small, inconspicuous font and is listed among many other links at the bottom of the page.

22 57. Unlike first-party cookies that may be necessary to view a webpage, third-party
23 tracker cookies are not necessary. Moreover, they

- 24 (1) simultaneously communicate information to an external server as a user navigates a
25 website;
- 26 (2) track users across devices, meaning that a user’s actions on multiple devices all will be
27 included in the information stored regarding that user;
- 28 (3) are not easily disabled by users; and
- (4) *create a record of all of the information that users provide to and/or receive from the*

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

1 *website.*

2 58. Because they were unaware of Defendant’s use of third-party trackers and tracking
3 cookies, Plaintiffs and Class members could not and did not consent to the collection, storage, and
4 use of their personally identifying and addressing information by undisclosed third parties such as
5 Taboola, Amobee, and Xandr.

6 59. Plaintiffs and Class members had and have a reasonable expectation of privacy in
7 their interactions with the USA Today website and their user data, especially their personally
8 identifying information. This is even truer of Plaintiffs’ and Class members’ IP addresses, which
9 contain geolocation data that can be used to identify, track and target individuals in a very specific
10 way.

11 60. Privacy studies, such as those conducted by the *Pew Research Center*, show that
12 most Americans are concerned about how data is collected about them.¹⁷ Those privacy polls also
13 reflect that Americans consider one of the most important privacy rights to be the need for an
14 individual’s affirmative consent before a company collects and shares data regarding that customer
15 or other individual.

16 61. Indeed, according to *Consumer Reports*, more than 90% of Americans believe that
17 more should be done to ensure that companies protect consumers’ privacy. Further, a
18 supermajority of Americans – **64%** – believe that companies should be prohibited from sharing
19 data with third parties, while 63% of Americans want a federal law requiring companies to obtain
20 a consumer’s permission before sharing the consumer’s information. To that end, 60% of
21 Americans believe that companies should be required to be more transparent about their privacy
22 policies so that consumers can make more informed choices.¹⁸

23
24

25 ¹⁷ Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of*
26 *Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019),
[https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-
and-feeling-lack-of-control-over-their-personal-information/](https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/)

27 ¹⁸ Benjamin Moskowitz et al., *Privacy Front & Center: Meeting the Commercial Opportunity to*
28 *Support Consumer Rights*, Consumer Reports in collaboration with Omidyar Network (Fall 2020),
https://thedigitalstandard.org/downloads/CR_PrivacyFrontAndCenter_102020_vf.pdf

1 62. Users act in a manner that is consistent with those preferences. During a rollout of
2 new iPhone operating software, for example, *94% of U.S. users who were asked for clear,*
3 *affirmative consent before allowing companies to track them chose not to share their data.*¹⁹

4 63. Defendant's unauthorized (1) installation of third-party tracker cookies on
5 Plaintiffs' and Class members' web browsers and (2) collection and disclosure of Plaintiffs' and
6 Class members' personally identifying and addressing information to undisclosed third parties,
7 without consent or adequate notification, are invasions of Plaintiffs' and Class members' privacy.

8 64. Plaintiffs and Class members have suffered injuries in the form of (i) invasion of
9 privacy; (ii) statutory damages; (iii) the continued and ongoing risk to their personally identifying
10 information that, once out, cannot be restored to its previous level of privacy; and (iv) the continued
11 and ongoing risk of harassment, spam, and targeted advertisements enabled by the USA Today
12 website.

CLASS ACTION ALLEGATIONS

13
14 65. Plaintiffs bring this action under California Code of Civil Procedure § 382 on behalf
15 of himself and a class (the "USA Today Website Class" or "the Class") defined as follows:

16 All California residents who, while located within California at any time during the
17 applicable limitations period preceding the original filing of the Complaint in this
18 matter and through and including the date of resolution, accessed and viewed the
19 USA Today website and had their IP addresses collected by and disclosed to the
20 third-party trackers embedded in the USA Today website.

21 66. Excluded from the USA Today Website Class are website users who (i) registered
22 for the USA Today smartphone application and/or (ii) subscribed to receive the USA Today
23 eNewspaper. Employees of Defendant and employees of Defendant's parents, subsidiaries, and
24 corporate affiliates also are excluded from the Class. Plaintiffs reserve the right to amend or
25 modify the class definition and/or to add sub-classes or limitations to particular issues, where

26
27 ¹⁹ See <https://www.wired.co.uk/article/apple-ios14-facebook> ("According to Flurry Analytics,
28 **85 per cent of worldwide users clicked 'ask app not to track' when prompted, with the proportion rising to 94 per cent in the US.**").

1 appropriate, based upon subsequently discovered information.

2 67. This action properly may be maintained as a class action under section 382 of the
3 California Code of Civil Procedure because (1) there is a well-defined community of interest in
4 the litigation, (2) common questions of law and fact predominate over individual issues, and (3)
5 the proposed Class is ascertainable.

6 **Numerosity**

7 68. The USA Today Website Class that Plaintiffs seek to represent contains numerous
8 members and is clearly ascertainable including, without limitation, by using Defendant's records
9 and/or third-party trackers' records to determine the size of the Class and to determine the identities
10 of individual Class members.

11 69. Based on information and belief, the USA Today Website Class consists of at least
12 75 individuals. The Class is so numerous that joinder of all members is impracticable.

13 **Typicality**

14 70. Plaintiffs' claims are typical of the claims of all the other members of the USA
15 Today Website Class, as Plaintiffs now suffer and have suffered from the same violations of the
16 law as other putative Class members. Plaintiffs' claims and the Class members' claims are based
17 on the same legal theories and arise from the same unlawful conduct, resulting in the same injury
18 to Plaintiffs and all of the other Class members.

19 **Adequacy**

20 71. Plaintiffs will fairly and adequately represent and protect the interests of the other
21 members of the Class. Plaintiffs have retained competent counsel with substantial experience in
22 prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to
23 prosecuting this action vigorously on behalf of the USA Today Website Class members and have
24 the financial resources to do so. Neither Plaintiffs nor their counsel have any interests that are
25 adverse to those of the other USA Today Website Class members.

26 **Commonality and Predominance**

27 72. By its unlawful actions, Defendant has violated Plaintiffs' and the Class members'
28 rights under the CDAFA, the CIPA and the California Constitution. The questions raised are,

1 therefore, of common or general interest to the Class members, who have a well-defined
2 community of interest in the questions of law and fact presented in this Complaint.

3 73. This action involves common questions of law and fact that predominate over any
4 questions affecting only individual Class members. Those common questions of law and fact
5 include, without limitation, the following:

- 6 (a) Whether Plaintiffs and Class members had a reasonable expectation of privacy
7 when they accessed and visited the USA Today website;
- 8 (b) Whether Defendant knowingly and without permission accessed Plaintiffs' and
9 Class members' computers;
- 10 (c) Whether Defendant knowingly and without permission altered, damaged, deleted,
11 destroyed, or otherwise used any data from Plaintiffs' and Class members'
12 computers;
- 13 (d) Whether Defendant knowingly and without permission took, copied, or made use
14 of any data from Plaintiffs' and Class members' computers;
- 15 (e) Whether Defendant knowingly and without permission added, altered, damaged,
16 deleted, or destroyed any data from Plaintiffs' and Class members' computers;
- 17 (f) Whether Plaintiffs and Class members had a reasonable expectation of privacy in
18 their personally identifying information, including IP addresses, when they
19 accessed and visited the USA Today website;
- 20 (g) Whether each of the third-party trackers embedded in the USA Today website is a
21 "pen register" under California Penal Code § 638.50(b);
- 22 (h) Whether Defendant has or had a policy or practice of collecting and sharing
23 personally identifying and addressing information collected on the USA Today
24 website including, without limitation, IP addresses, with third-party trackers and/or
25 other third parties;
- 26 (i) Whether Defendant has or had a policy or practice of not disclosing to USA Today
27 website users that it would collect and share their personally identifying and
28

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

- 1 addressing information, including IP addresses, with third-party trackers and/or
2 other third parties;
- 3 (j) Whether Defendant has or had a policy or practice of not obtaining USA Today
4 website users' prior consent to collect and share personally identifying and
5 addressing information, including IP addresses, with third-party trackers and/or
6 other third parties;
- 7 (k) Whether Defendant sought or obtained a court order for its use of the third-party
8 trackers;
- 9 (l) Whether Defendant's conduct invaded Plaintiffs' and Class members' privacy;
- 10 (m) Whether Defendant's acts and practices violate or violated California's Computer
11 Data Access and Fraud Act, Cal. Penal Code § 502;
- 12 (n) Whether Defendant's acts and practices violate or violated the California Invasion
13 of Privacy Act, Cal. Penal Code § 638.51(a);
- 14 (o) Whether Defendant's acts and practices violate or violated the California
15 Constitution or individual rights arising under the California Constitution; and
- 16 (p) Whether Plaintiffs and Class members are entitled to actual, statutory, nominal,
17 and/or other forms of damages, restitution, and other relief.

18 **Superiority**

19 74. A class action is superior to other available methods for the fair and efficient
20 adjudication of this controversy because individual litigation of the claims of all of the members
21 of the Class is impracticable and because questions of law and fact common to the USA Today
22 Website Class predominate over any questions affecting only individual members of the Class.
23 Even if every individual member of the Class could afford individual litigation, the court system
24 could not. It would be unduly burdensome to the courts if individual litigation of the numerous
25 cases were to be required. Individualized litigation also would present the potential for varying,
26 inconsistent or contradictory judgments and would magnify the delay and expense to all parties
27 and to the court system resulting from multiple trials of the same factual issues. By contrast, the
28 conduct of this action as a class action with respect to some or all of the issues will present fewer

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

1 management difficulties, conserve the resources of the court system and the parties, and protect
2 the rights of each member of the USA Today Website Class. Further, it will prevent the very real
3 harm that would be suffered by numerous members of the putative Class who simply will be unable
4 to enforce individual claims of this size on their own, and by Defendant’s competitors, who will
5 be placed at a competitive disadvantage as their punishment for obeying the law. Plaintiffs
6 anticipate no difficulty in the management of this case as a class action.

7 75. The prosecution of separate actions by individual members of the USA Today
8 Website Class would create a risk of adjudications with respect to them that would, as a practical
9 matter, be dispositive of the interests of other members of the Class who are not parties to those
10 adjudications or that would substantially impair or impede the ability of those non-party members
11 of the Class to protect their interests.

12 76. The prosecution of individual actions by members of the USA Today Website Class
13 also would run the risk of establishing inconsistent standards of conduct for Defendant.

14 **FIRST CAUSE OF ACTION**
15 **Violation of the California Computer Data Access and Fraud Act**
16 **(California Penal Code § 502)**

17 77. Plaintiffs incorporate each allegation set forth above as if fully set forth herein and
18 further alleges as follows.

19 78. The California Legislature enacted the CDAFA with the intent to “expand the
20 degree of protection afforded to individuals, businesses, and governmental agencies from
21 tampering, interference, damage, and unauthorized access to lawfully created computer data and
22 computer systems.” Cal. Penal Code § 502(a).

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

28 80. 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

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

1 with, or communicate with, the logical, arithmetical, or memory function resources of a computer,
2 computer system, or computer network.” Cal. Penal Code § 502(b)(1).

3 81. The term “computer program or software” is defined as “a set of instructions or
4 statements, and related data, that when executed in actual or modified form, cause a computer,
5 computer system, or computer network to perform specified functions.” Cal. Penal Code §
6 502(b)(3).

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

12 83. Plaintiffs’ and Class members’ web browsers used to access the USA Today
13 website are “computer software,” and the computers on which Plaintiffs and Class members used
14 their web browsers constitute computers or “computer systems” within the scope of the CDAFA.

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

19 85. As discussed above, a website cookie, including a third-party tracker cookie, and
20 an IP address both are “data” within the meaning of the statute.

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

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

28 88. The CDAFA further prohibits any person from knowingly accessing and without

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

1 permission adding, altering, damaging, or destroying any data, computer software, or computer
2 programs which reside or exist internal or external to a computer, computer system, or computer
3 network. Cal. Penal Code § 502(c)(4).

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

8 90. Based on Defendant’s unauthorized installation and storage of third-party tracker
9 cookies on Plaintiffs’ and Class members’ web browsers, as alleged above, Defendant knowingly
10 accessed and without permission altered and used Plaintiffs’ and Class members’ data and
11 computer systems in violation of Penal Code § 502(c)(1).

12 91. Similarly, the installation of those third-party tracker cookies violates subsection
13 (c)(4) because Defendant added and altered data and computer software on Plaintiffs’ and Class
14 members’ computers or computer systems. Cal. Penal Code § 502(c)(4).

15 92. By installing third-party tracker cookies, Defendant also knowingly and without
16 permission provided those trackers a means of accessing and/or caused to be accessed Plaintiffs’
17 and Class members’ computers, computer systems, and/or computer networks in violation of Penal
18 Code §§ 502(c)(6) and (7).

19 93. Further, Defendant’s unauthorized collection and disclosure to undisclosed third
20 parties of Plaintiffs’ and Class members’ personally identifying and addressing information
21 violates Penal Code § 502(c)(2) because Defendant took and made use of data, including IP
22 addresses, from Plaintiffs’ and Class members’ computers, computer systems, or computer
23 networks.

24 94. Plaintiffs and Class members are residents of California who used their computers,
25 computer systems, and/or computer networks in California. Defendant accessed or caused to be
26 accessed Plaintiffs’ and Class members’ data and other personally identifying information from
27 within California.

28 95. Defendant was unjustly enriched by accessing, acquiring, taking, and using

1 Plaintiffs’ and Class members’ data and computer systems without their permission or consent,
 2 and using all of that identifying information to maximize revenue from selling advertising space
 3 on the USA Today website and for Defendant’s own financial benefit. Defendant has been unjustly
 4 enriched in an amount to be determined at trial.

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

9 97. Plaintiffs and Class members also are entitled to an award of reasonable attorneys’
 10 fees and costs under Penal Code § 502(e)(2).

11 **SECOND CAUSE OF ACTION**
 12 **Unlawful Use of a Pen Register or Trap and Trace Device**
 13 **(California Penal Code § 638.51)**

14 98. Plaintiffs incorporate each allegation set forth above as if fully set forth herein and
 15 further alleges as follows.

16 99. The California Legislature enacted the California Invasion of Privacy Act, Cal.
 17 Penal Code §§ 630, *et seq.* (“CIPA”), to address “advances in science and technology [that] have
 18 led to the development of new devices and techniques for the purpose of eavesdropping upon
 19 private communications” and declared “that the invasion of privacy resulting from the continual
 20 and increasing use of such devices and techniques has created a serious threat to the free exercise
 21 of personal liberties and cannot be tolerated in a free and civilized society.” *Id.* § 630. CIPA is
 22 intended “to protect the right of privacy of the people of this state.” *Id.*

23 100. Although CIPA was enacted before the dawn of the Internet, the California
 24 Supreme Court “regularly reads statutes to apply to new technologies where such a reading would
 25 not conflict with the statutory scheme.” *In re Google Inc.*, 2013 WL 5423918, at *21 (N.D. Cal.
 26 Sept. 26, 2013); *see also Greenley*, 2023 WL 4833466, at *15 (referencing CIPA’s “expansive
 27 language” when finding that software was a “pen register”); *Javier v. Assurance IQ, LLC*, 2022
 28 WL 1744107, at *1 (9th Cir. May 31, 2022) (“Though written in terms of wiretapping, [CIPA]
 Section 631(a) applies to Internet communications.”). This is consistent with the observation in

1 *Matera v. Google Inc.* that, “when faced with two possible interpretations of CIPA, the California
2 Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest
3 privacy protection.” *Matera v. Google Inc.*, 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

4 101. Particularly pertinent here, *California Penal Code § 638.51(a) makes it unlawful*
5 for a person *to “install or use a pen register or a trap and trace device* without first obtaining a
6 court order.”

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

11 103. A “trap and trace device” is a “a device or process that captures the incoming
12 electronic or other impulses that identify the originating number or other dialing, routing,
13 addressing, or signaling information reasonably likely to identify the source of a wire or electronic
14 communication, but not the contents of a communication.” Cal. Penal Code § 638.50(c).

15 104. In essence, a “pen register” is a “device or process” that records *outgoing*
16 information, while a “trap and trace device” is a “device or process” that records *incoming*
17 information. For example, if a user sends an email, a “pen register” might record the email address
18 from which the email was sent, the email address to which the email was sent, and the subject line
19 – because this is the user’s *outgoing* information. On the other hand, if that same user receives an
20 email, a “trap and trace device” might record the email address from which that email was sent,
21 the email address to which it was sent, and the subject line – because this is *incoming* information
22 that is being sent to that same user.

23 105. The three trackers embedded in the USA Today website – Taboola, Amobee, and
24 Adnx – are “pen registers” because each of them is a device or process that captures and records
25 outgoing addressing or signaling information from the electronic communications transmitted by
26 Plaintiffs’ and Class members’ computers, computer systems, and computer networks as they are
27 accessing and visiting the USA Today website.

28 106. At all relevant times, Defendant installed and is installing each of the three pen

1 register trackers on Plaintiffs’ and Class members’ web browsers and used the trackers to collect
 2 Plaintiffs’ and Class members’ outgoing IP addresses. IP addresses constitute addressing
 3 information and do not necessarily reveal any more about the underlying contents of the
 4 communication. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1108 (9th Cir. 2014).

5 107. Unaware of Defendant’s installation and use of the third-party trackers as pen
 6 registers, Plaintiffs and Class members could not have provided and did not provide their prior
 7 consent to Defendant’s installation or use of the third-party trackers or pen registers.

8 108. Upon information and belief, Defendant was not authorized by any court order to
 9 use a pen register to track Plaintiffs’ and Class members’ location data and other identifying or
 10 addressing information.

11 109. Defendant’s conduct as described above violated California Penal Code § 638.51.
 12 As a result, Defendant is liable for the relief sought by Plaintiffs and the USA Today Website
 13 Class. Under California Penal Code § 637.2, Plaintiffs and Class Members are entitled to and seek
 14 statutory damages of \$5,000 for each of Defendant’s numerous CIPA violations.

THIRD CAUSE OF ACTION

Invasion of Privacy

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

15
 16
 17 110. Plaintiffs incorporate each allegation set forth above as if fully set forth herein and
 18 further alleges as follows.

19 111. “Privacy” is listed in Article I, Section 1, of the California Constitution as a
 20 fundamental right of all Californians. That section of the Constitution provides as follows: “All
 21 people are by nature free and independent and have inalienable rights. Among these are enjoying
 22 and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and
 23 obtaining safety, happiness, and privacy.” Cal. Const. art. I, § 1.

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

1 113. Plaintiffs and Class members have a legally protected privacy interest in their
2 personally identifying information and addressing information that are captured, without notice or
3 consent, when they access and view the USA Today website. These privacy interests are
4 recognized by the California Constitution, CDAFA, CIPA, HIPAA, and numerous other statutes.

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

12 115. Defendant's unauthorized (1) installation of third-party tracker cookies and (2)
13 collection and disclosure to undisclosed third parties of Plaintiffs' and Class members' personally
14 identifying and addressing information, all without consent or adequate notification to Plaintiffs
15 and Class members, are invasions of Plaintiffs' and Class members' privacy.

16 116. Defendant's conduct constituted a serious invasion of privacy that would be highly
17 offensive to a reasonable person in that (i) the information disclosed by Defendant and shared with
18 third-party trackers was personally identifying information protected by the California
19 Constitution and numerous California and federal statutes; (ii) Defendant did not have
20 authorization or consent to disclose that personally identifying and addressing information,
21 including IP addresses, to any third-party tracker embedded in the USA Today website, and the
22 trackers did not have authorization to collect and use that geolocation information; and (iii) the
23 invasion deprived Plaintiffs and Class members of the ability to control the dissemination and
24 circulation of that information, an ability that is considered a fundamental privacy
25 right. Defendant's conduct constitutes a severe and egregious breach of social norms.

26 117. As a direct and proximate result of Defendant's actions, Plaintiffs and Class
27 members have had their privacy invaded and have sustained injury, including injury to their peace
28 of mind.

1 118. Plaintiffs and USA Today Website Class members seek appropriate relief for that
2 injury, including but not limited to restitution, disgorgement of profits earned by Defendant
3 because of, by way of or in connection with the intrusions upon Plaintiffs' and Class members'
4 privacy, nominal damages, and all other equitable relief that will compensate Plaintiffs and Class
5 members properly for the harm to their privacy interests.

6 119. Plaintiffs also seek such other relief as the Court may deem just and proper.

7 **PRAYER FOR RELIEF**

8 **WHEREFORE**, Plaintiffs, on behalf of themselves and the members of the Class, prays
9 for the following relief:

- 10 a. An order certifying the USA Today Website Class, appointing Plaintiffs Ryan Wu
11 and Saber Khamooshi as representatives of the USA Today Website Class, and
12 appointing counsel for Plaintiffs as counsel for the USA Today Website Class;
- 13 b. An order declaring that Defendant's actions, as described above, violate California
14 Penal Code § 502;
- 15 c. An order declaring that Defendant's actions, as described above, violate California
16 Penal Code § 638.51;
- 17 d. An order declaring that Defendant's actions, as described above, violate Art. 1, § 1
18 of the California Constitution;
- 19 e. A judgment for and award of compensatory damages or other equitable relief under
20 California Penal Code § 502(e)(1) to Plaintiffs and each of the members of the USA
21 Today Website Class;
- 22 f. A judgment for and award of statutory damages of \$5,000 per violation of CIPA
23 under California Penal Code § 637.2 to Plaintiffs and each of the members of the
24 USA Today Website Class;
- 25 g. A judgment for and award of restitution, disgorgement of profits, and nominal
26 damages to which Plaintiffs and each of the members of the USA Today Website
27 Class are entitled by law;
- 28 h. Payment of costs of the suit;

- 1 i. Payment of attorneys' fees under California Code of Civil Procedure § 1021.5 and
- 2 Penal Code § 502(e)(2);
- 3 j. An award of pre- and post-judgment interest to the extent allowed by law; and
- 4 k. Such other and further relief as the Court may deem proper.

5
6 Respectfully submitted,

7 Dated: July 23, 2024

KELLER GROVER LLP

8
9 By: 

ERIC A. GROVER
Attorneys for Plaintiff

10
11
12
13 **JURY DEMAND**

14
15 Plaintiffs request a trial by jury of all claims that can be so tried.

16
17
18 Respectfully submitted,

19 Dated: July 23, 2024

KELLER GROVER LLP

20
21 By: 

ERIC A. GROVER
Attorneys for Plaintiff

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [USAToday.com Unlawfully Collects Visitor Info via Secret Tracking Software, Class Action Lawsuit Alleges](#)
