

GUTRIDE SAFIER LLP

Seth A. Safier (State Bar No. 197427)

seth@gutridesafier.com

Marie A. McCrary (State Bar No. 262670)

marie@gutridesafier.com

Todd Kennedy (State Bar No. 250267)

todd@gutridesafier.com

100 Pine Street, Suite 1250

San Francisco, CA 94111

Telephone: (415) 639-9090

Facsimile: (415) 449-6469

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MARTIN BELTRAN, as an individual, on
behalf of himself, the general public, and those
similarly situated,

Plaintiff,

v.

KOHLER CO.,

Defendant.

CASE NO.

CLASS ACTION COMPLAINT FOR
INVASION OF PRIVACY; INTRUSION
UPON SECLUSION; WIRETAPPING IN
VIOLATION OF THE CALIFORNIA
INVASION OF PRIVACY ACT
(CALIFORNIA PENAL CODE § 631); USE
OF A PEN REGISTER IN VIOLATION OF
THE CALIFORNIA INVASION OF
PRIVACY ACT (CALIFORNIA PENAL
CODE § 638.51); COMMON LAW FRAUD,
DECEIT AND/OR
MISREPRESENTATION; and UNJUST
ENRICHMENT

JURY TRIAL DEMANDED

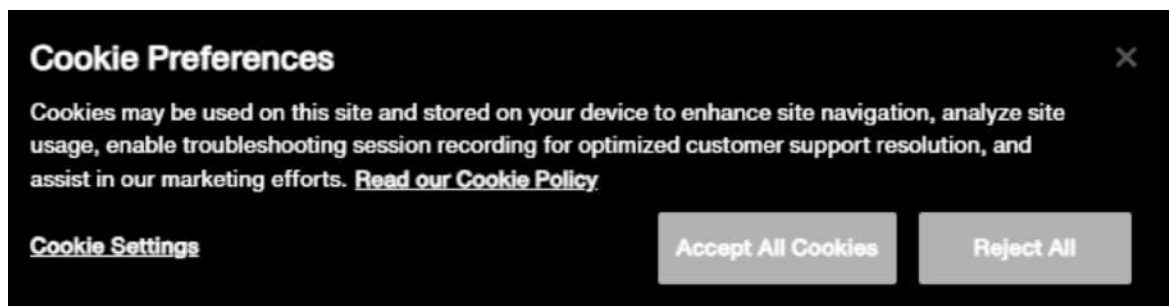
TABLE OF CONTENTS

1		
2	INTRODUCTION	3
3	THE PARTIES.....	4
4	JURISDICTION AND VENUE	5
5	SUBSTANTIVE ALLEGATIONS	5
6	A. Defendant Programmed the Websites to Include Third-Party Resources that	
7	Utilize Cookie Trackers.	5
8	B. Defendant Falsely Informed Users That They Could Reject the Websites’ Use of	
9	“All” Cookies.....	10
10	C. The Private Communications Collected As a Result of Third Party Cookies	
11	Transmitted When Visiting Defendant’s Websites.....	15
12	1. The Websites Cause the Interception of the Contents of Communications	
13	15
14	2. Facebook Cookies (Kohler, Robern, and Kallista Websites)	16
15	3. TikTok Cookies (Kohler Website).....	24
16	4. Microsoft Clarity Cookies (Kohler Website).....	29
17	D. The Private Communications Collected are Valuable.	31
18	PLAINTIFFS’ EXPERIENCES	33
19	CLASS ALLEGATIONS	35
20	CAUSES OF ACTION.....	37
21	First Cause of Action: Invasion of Privacy.....	37
22	Second Cause of Action: Intrusion Upon Seclusion.....	40
23	Third Cause of Action: Wiretapping in Violation of the California Invasion of Privacy	
24	Act (California Penal Code § 631).....	42
25	Fourth Cause of Action: Use of a Pen Register in Violation of the California Invasion of	
26	Privacy Act (California Penal Code § 638.51)	46
27	Fifth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation.....	48
28	PRAYER FOR RELIEF	50

Plaintiff Martin Beltran (“Plaintiff”) brings this action on behalf of himself, the general public, and all others similarly situated against Kohler Co. (“Defendant” or “Kohler”). Plaintiff’s allegations against Defendant are based upon information, belief and upon investigation of Plaintiff’s counsel, except for allegations specifically pertaining to Plaintiff, which are based upon Plaintiff’s personal knowledge.

INTRODUCTION

1. This Class Action Complaint concerns an egregious privacy violation and total breach of consumer trust in violation of California law. When consumers visit Defendant’s ecommerce websites (<https://www.kohler.com>, the “Koller Website”; <https://www.robern.com>, the “Robern Website”; and <https://www.kallista.com>, the “Kallista Website”; each a “Website” and collectively, the “Websites”), Defendant displays to them a popup cookie consent banner. Defendant’s cookie banners each disclose that the Website uses cookies but expressly gives users the option to control how they are tracked and how their personal data is used. Defendant assures visitors that they can choose to “Reject All” cookies, as shown in the following screenshot:



2. Like most internet websites, Defendant designed the Websites to include resources and programming scripts from third parties that cause those parties to place cookies and other similar tracking technologies on visitors’ browsers and devices and/or transmit cookies along with user data. However, unlike other websites, Defendant’s Websites offer consumers a choice to browse without being tracked, followed, and targeted by third party data brokers and advertisers. But Defendant’s promises are outright lies, designed to lull users into a false sense of security. Even after users elect to “Reject All” cookies, Defendant surreptitiously causes several third parties—including Meta Platforms, Inc. (Facebook), ByteDance Ltd. (TikTok),

1 Microsoft Corporation (Microsoft Clarity), and others (the “Third Parties”) —to place and/or
2 transmit cookies that track users’ website browsing activities and eavesdrop on users’ private
3 communications on the Websites.

4 3. Contrary to their express rejection of cookies and tracking technologies on the
5 Websites, Defendant nonetheless caused cookies, including the Third Parties’ cookies, to be sent
6 to Plaintiff’s and other visitors’ browsers, stored on their devices, and transmitted to the Third
7 Parties along with user data. These third-party cookies permitted the Third Parties to track and
8 collect data in real time regarding the behaviors and communications of visitors to the Websites,
9 including their browsing history, visit history, website interactions, user input data, demographic
10 information, interests and preferences, shopping behaviors, device information, referring URLs,
11 session information, user identifiers, and/or geolocation data—including whether a user is
12 located in California.

13 4. The Third Parties analyze and aggregate this user data across websites and time
14 for their own purposes and financial gain, including, creating consumer profiles containing
15 detailed information about a consumer’s behavior, preferences, and demographics; creating
16 audience segments based on shared traits (such as Millennials, Californians, tech enthusiasts,
17 etc.); and performing targeted advertising and marketing analytics. Further, the Third Parties
18 share user data and/or user profiles to unknown parties to further their financial gain.

19 5. This type of tracking and data sharing is exactly what the Website visitors who
20 clicked or selected the “Reject All” button on any of the Websites’ cookie consent banners sought
21 to avoid. Defendant falsely told users of the Websites that it respected their privacy and that they
22 could avoid tracking and data sharing when they browsed the Websites. Despite receiving notice
23 of consumers’ express declination of consent, Defendant defied it and violated state statutes and
24 tort duties owed to Plaintiff and those similarly situated users of the Websites.

25 **THE PARTIES**

26 6. Plaintiff Martin Beltran is, and was at all relevant times, an individual and
27 resident of San Francisco, California. Plaintiff Beltran intends to remain in California and makes
28 his permanent home there.

7. Defendant Kohler Co. is a Wisconsin corporation with its headquarters and principal place of business in Kohler, Wisconsin.

JURISDICTION AND VENUE

8. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332(d)(2). The aggregate amount in controversy exceeds \$5,000,000, exclusive of interest and costs; and Plaintiff and Defendant are citizens of different states.

9. The injuries, damages and/or harm upon which this action is based, occurred or arose out of activities engaged in by Defendant within, affecting, and emanating from, the State of California. Defendant regularly conducts and/or solicits business in, engages in other persistent courses of conduct in, and/or derives substantial revenue from products and services provided to persons in the State of California. Defendant has engaged, and continues to engage, in substantial and continuous business practices in the State of California.

10. Further, the Private Communications and data which Defendant causes to be transmitted to Third Parties are routed through servers located in California.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in the state of California, including within this District.

12. Plaintiff accordingly alleges that jurisdiction and venue are proper in this Court.

SUBSTANTIVE ALLEGATIONS

A. Defendant Programmed the Websites to Include Third-Party Resources that Utilize Cookie Trackers.

13. Every website, including each of the Websites, is hosted by a server that sends and receives communications in the form of HTTP requests, such as “GET” or “POST” requests, to and from Internet users’ browsers. For example, when a user clicks on a hyperlink on the Website, the user’s browser sends a “GET” request to the Website’s server. The GET request tells the Website’s server what information is being requested (e.g., the URL of the webpage being requested) and instructs the Website’s server to send the information back to the user (e.g., the content of the webpage being requested). When the Website’s server receives an HTTP

1 request, it processes that request and sends back an HTTP response. The HTTP request includes
2 the client's IP address so that the Website's server knows where to send the HTTP response.

3 14. An IP address (Internet Protocol address) is a unique numerical label assigned to
4 each device connected to a network that uses the Internet Protocol for communication, typically
5 expressed as four sets of numbers separated by periods (e.g., 192.168.123.132 for IPv4
6 addresses). IP addresses can identify the network a device is on and the specific device within
7 that network. Public IP addresses used for internet-facing devices reveal geographical locations,
8 such as country, city, or region, through IP geolocation databases.

9 15. As a result, Defendant knew that the devices used by Plaintiff and Class members
10 to access the Websites were located in California.

11 16. Defendant voluntarily integrated "third-party resources" from the Third Parties
12 into its Websites' programming. "Third-party resources" refer to tools, content or services
13 provided by third-parties, such as analytics tools, advertising networks, or payment processors,
14 that a website developer utilizes by embedding scripts, styles, media, or application
15 programming interface (API) into the website's code. Defendant's use of the third-party
16 resources on the Websites is done so pursuant to agreements between Defendant and those Third
17 Parties.

18 17. The Websites cause users' devices to store and/or transmit both first-party and
19 third-party tracking cookies. Cookies are small text files sent by a website server to a user's web
20 browser and stored locally on the user's device. As described below, cookies generally contain
21 a unique identifier which enables the website to recognize and differentiate individual users.
22 Cookie files are sent back to the website server along with HTTP requests, enabling the website
23 to identify the device making the requests, and to record a session showing how the user interacts
24 with the website.

25 18. First-party cookies are those that are placed on the user's device directly by the
26 web server with which the user is knowingly communicating (in this case, the Website's server).
27 First-party cookies are used to track users when they repeatedly visit the same website.
28

1 19. A third-party cookie is set by a third-party domain/webserver (e.g.,
2 www.facebook.com; analytics.tiktok.com; d.clarity.ms, etc.) When the user's browser loads a
3 webpage (such as a webpage of the Website) containing embedded third-party resources, the
4 third-parties' programming scripts typically issue HTTP commands to determine whether the
5 third-party cookies are already stored on the user's device and to cause the user's browser to
6 store those cookies on the device if they do not yet exist. Third-party cookies include an identifier
7 that allows the third-party to recognize and differentiate individual users across websites
8 (including the Website) and across multiple browsing sessions.

9 20. As described further below, the third-party cookies stored on and/or loaded from
10 users' devices when they interact with the Websites are transmitted to those third parties,
11 enabling them to surreptitiously track in real time and collect Website users' personal
12 information, such as their browsing activities and private communications with Defendant,
13 including the following:

- 14 • **Browsing History:** Information about the webpages a Website user visits,
15 including the URLs, titles, and keywords associated with the webpages viewed,
16 time spent on each page, and navigation patterns;
- 17 • **Visit History:** Information about the frequency and total number of visits to the
18 Website;
- 19 • **Websites Interactions:** Data on which links, buttons, or ads on the Websites that
20 a user clicks;
- 21 • **User Input Data:** The information the user entered into the Websites' form
22 fields, including search queries, the user's name, age, gender, email address,
23 location, and/or payment information;
- 24 • **Demographic Information:** Inferences about age, gender, and location based on
25 browsing habits and interactions with Websites content;
- 26 • **Interests and Preferences:** Insights into user interests based on the types of
27 Websites content viewed, products searched for, or topics engaged with;
- 28

- 1 • **Shopping Behavior:** Information about the Websites products viewed or added
- 2 to shopping carts;
- 3 • **Device Information:** Details about the Websites user’s device, such as the type
- 4 of device (mobile, tablet, desktop), operating system, and browser type;
- 5 • **Referring URL:** Information about the website that referred the user to the
- 6 Website;
- 7 • **Session Information:** Details about the user’s current Websites browsing
- 8 session, including the exact date and time of the user’s session, the session
- 9 duration and actions taken on the Websites during that session;
- 10 • **User Identifiers:** A unique ID that is used to recognize and track a specific
- 11 Websites user across different websites over time; and/or
- 12 • **Geolocation Data:** General location information based on the Websites user’s IP
- 13 address or GPS data, if accessible, including whether the user is located in
- 14 California.

15 (Collectively, the browsing activities and private communications listed in the bullet points
16 above shall be referred to herein as “Private Communications”).

17 21. Third-party cookies can be used for a variety of purposes, including (i) analytics
18 (e.g., tracking and analyzing visitor behavior, user engagement, and effectiveness of marketing
19 campaigns); (ii) personalization (e.g., remembering a user’s browsing history and purchase
20 preferences to enable product recommendations); (iii) advertising/targeting (e.g., delivering
21 targeted advertisements based on the user’s consumer profile (i.e., an aggregated profile of the
22 user’s behavior, preferences, and demographics); and (iv) social media integration (e.g.,
23 enabling sharing of users’ activities with social media platforms). Ultimately, third-party cookies
24 are utilized to boost website performance and revenue through the collection, utilization, and
25 dissemination of user data.

26 22. Defendant manufactures and sells, among other consumer products, plumbing
27 fixtures (sinks, toilets, faucets, and tubs) and bath & kitchen products. Defendant owns and
28 operates the Websites, which allows visitors to receive information about its products and

1 purchase products. As they interact with the Websites (e.g., by entering data into forms, clicking
 2 on links, and making selections), users of the Websites communicate Private Communications
 3 to Defendant, including their browsing history, visit history, website interactions, user input data,
 4 demographic information, interests and preferences, shopping behaviors, device information,
 5 referring URLs, session information, user identifiers, and/or geolocation data—including
 6 whether a user is located in California.

7 23. Defendant chose to install or integrate its Websites with resources from the Third
 8 Parties that, among other things, use cookies. Thus, when consumers visit the Websites, both
 9 first-party cookies and third-party cookies are placed on their devices and/or transmitted. This is
 10 caused by software code that Defendant incorporates into its Websites, or that Defendant causes
 11 to be loaded. Because Defendant controls the software code of its Websites, and is capable of
 12 determining whether a user is accessing any of the Websites from California, it has complete
 13 control over whether first-party and third-party cookies are placed on its California users'
 14 devices and/or transmitted to third parties.

15 24. Defendant explained the third-party cookies it used on the Kohler Website as
 16 follows in its Cookie Policy:

17 **What is a cookie?**

18 A cookie is a small text file that a website saves on your computer or mobile device
 19 when you visit the website. Cookies are then sent back to the originating website
 20 on each subsequent visit, or to another website that recognizes that cookie, to
 21 develop a record of the user's online activity. Cookies on this site may be delivered
 22 in a first-party (set by the Kohler website) or third-party (set by another website)
 context and may also be set in association with emails you receive from us. Cookies
 help us enhance your experience when using the Site. They also help us understand
 how people use our site, such as which pages are most popular, so that we can better
 serve Site users.

23 **Cookie Categories Used On This Site:**

24 **Category 1: strictly necessary cookies**

25 Category 1 cookies are essential in order to enable you to move around this Site
 26 and use its features, such as accessing secure areas of this Site. Without these
 27 cookies, services you have asked for, like shopping carts or e-billing, cannot be
 provided. These cookies do not gather information about you that could be used for
 marketing purposes and do not remember where you have been on the internet. This
 category of cookies cannot be disabled.

28 **Category 2: performance cookies**

Category 2 cookies collect information about how visitors use this Site, for instance which pages visitors go to most often, and if they get error messages from web pages. These cookies do not collect information that specifically identifies a visitor. All of the information that these cookies collect is aggregated and therefore anonymous. Such information is only used to improve how the Site works. Category 2 cookies only collect information about Site usage for the benefit of the Site operator.

Category 3: functionality cookies

Category 3 cookies allow this Site to remember choices you make (such as your user name, language or the region you are in) and provide enhanced, more personal or customized features. For instance, this Site may be able to provide you with local or regional product information by storing the region in which you are currently located in a cookie. These cookies can also be used to remember changes you have made to text size, fonts and other parts of the Site that you can customize. They may also be used to provide services you have asked for such as watching a video or commenting on a blog. The information these cookies collect may be anonymized and these cookies cannot track your browsing activity on other websites.

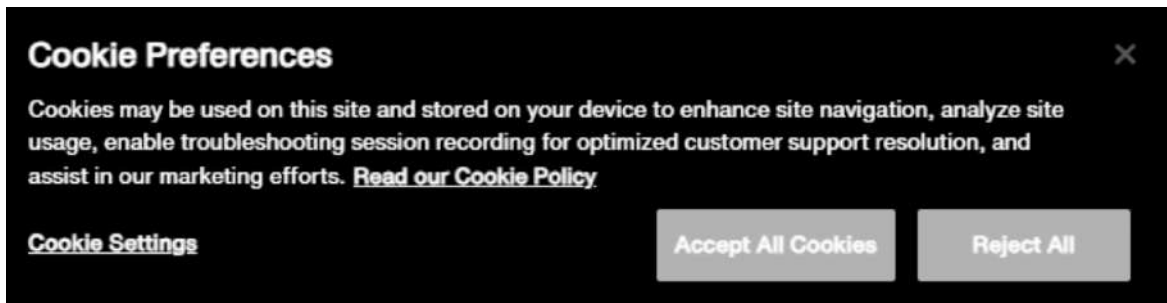
Category 4: targeting cookies or advertising cookies

Category 4 cookies are used to deliver advertisements that are more relevant to you and your interests. They are also used to limit the number of times you see an advertisement as well as help us measure the effectiveness of the advertising campaign. They are usually placed on your device by third-party advertising networks, but with our permission. These cookies remember that you have visited this Site. This information is shared with other organizations such as other third-party advertisers, and will be linked to website functionality provided by other organizations. To be clear, Category 4 cookies collect the most information about users. You may set your browser to opt-out or block these cookies.¹

B. Defendant Falsely Informed Users That They Could Reject the Websites' Use of "All" Cookies.

25. When Plaintiff and other consumers in California visited any of the Websites, the Website immediately displayed to them a popup cookie consent banner. As shown in the screenshot below, the cookie consent banner, titled "Cookie Preferences[.]" stated, "Cookies may be used on this site and stored on your device to enhance site navigation, analyze site usage, enable troubleshooting session recording for optimized customer support resolution, and assist in our marketing efforts." The banner then purported to provide users the opportunity to either "Accept All Cookies" or to instead "Reject All" cookies by clicking or selecting the button to do so, as shown in the following screenshot from the Website:

¹ Kohler Websites Cookie Policy (available at <https://www.kohler.com/en/legal/cookie-policy>) (the "Cookie Policy").



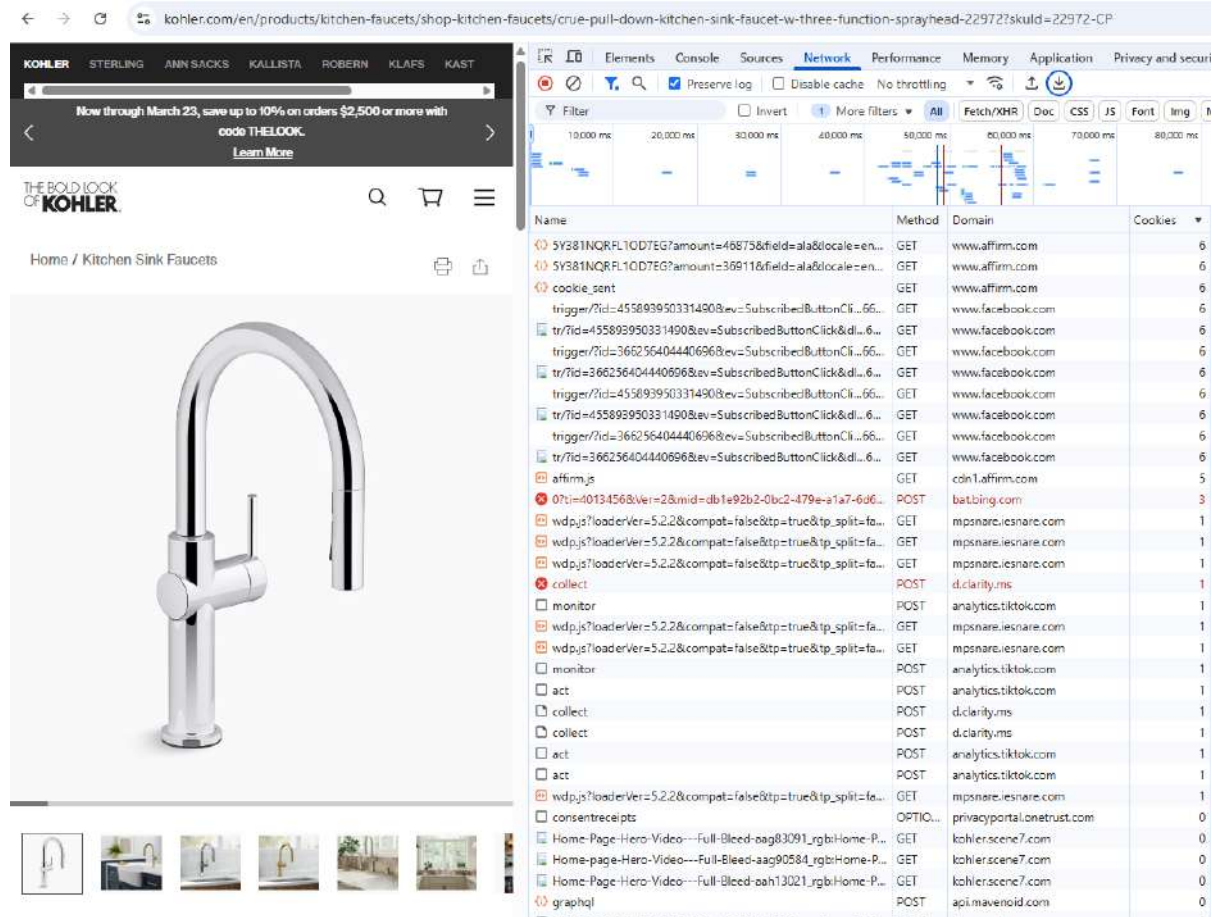
26. Plaintiff and other Website users who clicked or selected the “Reject All” button, thereby indicating their choice and/or agreement to decline or reject all cookies and tracking technologies in use on the Websites, could then continue to browse the Websites, as the popup cookie consent banner disappeared.

27. Defendant’s popup cookie consent banner led Plaintiff, and all those users of the Websites similarly situated, to believe that they declined or rejected “All” cookies and tracking technologies, especially those used to “enhance site navigation, analyze site usage, enable troubleshooting session recording...and assist in our marketing efforts.” The banner further reasonably led Plaintiff and those users of the Websites similarly situated to believe that Defendant would not allow third parties, through cookies, to access their Private Communications with the Websites, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, upon clicking or selecting the “Reject All” button.

28. Defendant’s representations, however, were false. In truth, Defendant did not abide by Plaintiff’s or other users’ wishes. When Plaintiff and other users of the Websites clicked or selected the “Reject All” button, they provided notice to Defendant that they did not consent to the placement or transmission of third-party cookies that would allow those parties to obtain their Private Communications with the Websites. Nevertheless, Defendant caused the Third Parties’ tracking cookies to be placed on Website users’ browsers and devices and/or transmitted to the Third Parties along with user data.

1 29. In particular, when users clicked or selected the “Reject All” button, Defendant
2 nonetheless continued to cause the Third Parties’ cookies to be placed on users’ devices and/or
3 transmitted to the Third Parties along with user data, enabling them to collect user data in real
4 time that discloses the Private Communications of visitors of the Websites, including browsing
5 history, visit history, website interactions, user input data, demographic information, interests
6 and preferences, shopping behaviors, device information, referring URLs, session information,
7 user identifiers, and/or geolocation data. In other words, even when consumers like Plaintiff tried
8 to protect their privacy by rejecting “All” cookies, Defendant failed to prevent cookies from
9 being transmitted to Third Parties, enabling them to track user behavior and communications.

10 30. Some aspects of the operations of the Third Parties’ cookies on the Websites can
11 be observed using specialized tools that log incoming and outgoing Website network
12 transmissions. The following screenshot, obtained using one such tool, shows examples of the
13 Third Parties’ cookies being transmitted from a Kohler Website user’s device and browser to the
14 Third Parties even after the user clicked or selected the “Reject All” button on the Kohler
15 Website’s popup cookie consent banner.



31. The screenshot above shows the “Network” tab of Chrome Developer Tools, which contains a list of HTTP network traffic transmissions between the user’s browser and various third-party websites while the user visited and interacted with the Kohler Website at <https://www.kohler.com>. The screenshot depicts only network traffic occurring *after* the user rejected “All” cookies using the cookie banner. As shown above, despite the user’s rejection of “All” cookies, the user’s interactions with the Kohler Website resulted in the user’s browser making a large number of GET and POST HTTP requests to third party web domains like www.facebook.com, analytics.tiktok.com, d.clarity.ms, and others. As further shown in the right-hand column of the screenshot, the user’s browser sent cookies along with those HTTP requests to the third parties. This screenshot demonstrates that the Kohler Website caused third-party cookie data and users’ Private Communications to be transmitted to Third Parties, even after consumers declined or rejected all cookies and tracking technologies by clicking or

1 selecting the “Reject All” button. All of these network calls are made to the Third Parties without
2 the user’s knowledge, and despite the user’s rejection of “All” cookies.

3 32. Plaintiff’s and other Website users’ Private Communications, including their
4 browsing history, visit history, website interactions, user input data, demographic information,
5 interests and preferences, shopping behaviors, device information, referring URLs, session
6 information, user identifiers, and/or geolocation data, were surreptitiously obtained by the Third
7 Parties via these cookies.

8 33. As users interact with the Websites, even after clicking or selecting the “Reject
9 All” button, thereby declining or rejecting the use of cookies and similar technologies for usage
10 analytics, session recording, and marketing efforts, as well as the sale or sharing of the user’s
11 personal information with third parties for such functions, or other purposes, more data regarding
12 users’ behavior and communications are sent to third parties, alongside the cookie data. The
13 third-party cookies that Defendant wrongfully allows to be stored on users’ devices and
14 browsers, and to be transmitted to the Third Parties, cause the Third Parties to track and collect
15 data on users’ behaviors and communications, including Private Communications, on the
16 Websites. Because third-party cookies cause the Third Parties to track users’ behavior across the
17 Internet and across time, user data can be correlated and combined with other data sets to compile
18 comprehensive user profiles that reflect consumers’ behavior, preferences, and demographics
19 (including psychological trends, predispositions, attitudes, intelligence, abilities, and aptitudes).
20 These Third Parties monetize user profiles for advertising, sales, and marketing purposes to
21 generate revenue and target advertising to Internet users. Advertisers can gain deep
22 understanding of users’ behavioral traits and characteristics and target those users with
23 advertisements tailored to their consumer profiles and audience segments.

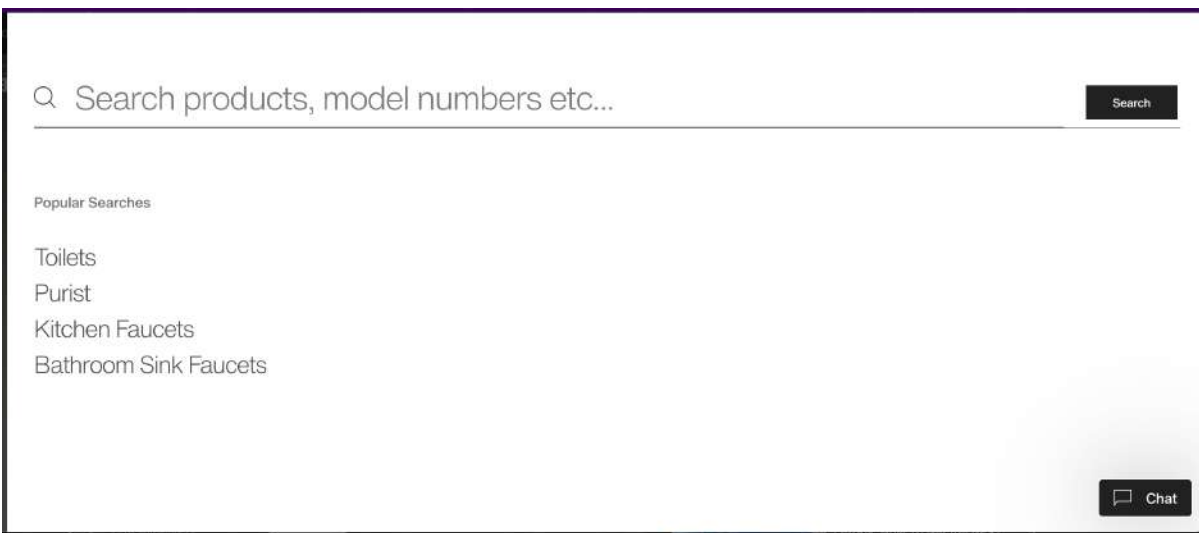
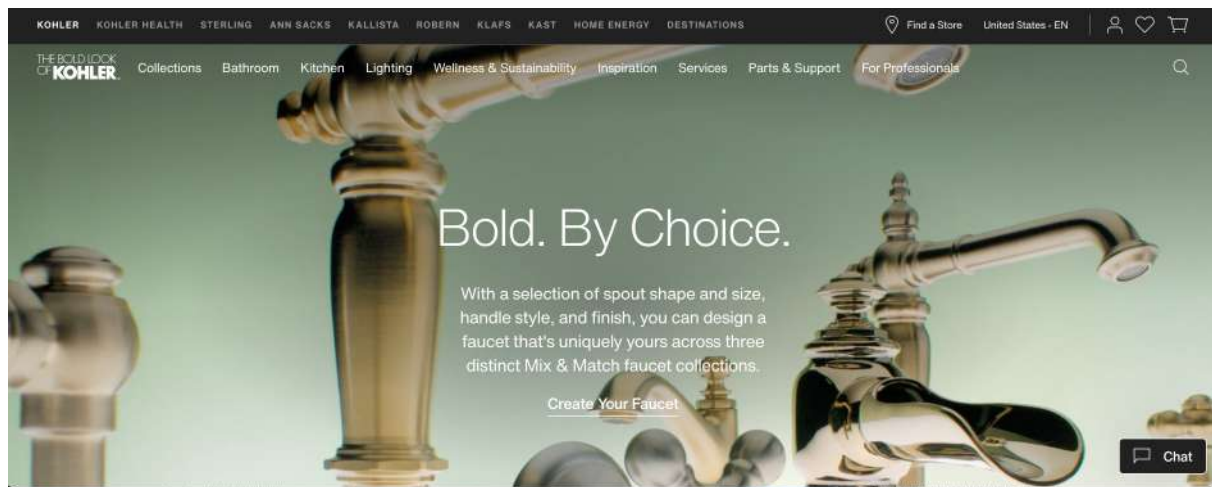
24 34. The Third Parties’ code that the Websites cause to be loaded and executed by the
25 user’s browser becomes a wiretap when it is executed because it causes the Third Parties—
26 separate and distinct entities from the parties to the conversations—to use cookies to eavesdrop
27 upon, record, extract data from, and analyze conversations to which they are not parties. When
28 the Third Parties use their respective wiretaps on Website users’ Private Communications, the

wiretaps are not like tape recorders or “tools” used by one party to record the other. The Third Parties each have the capability to use the contents of conversations they collect through their respective wiretaps for their own purposes as described in more detail below.

C. The Private Communications Collected As a Result of Third Party Cookies Transmitted When Visiting Defendant’s Websites.

1. The Websites Cause the Interception of the Contents of Communications

35. The Websites include search bars and forms where users input information. For example, below are screenshots of the search bar on the Kohler Website where users can type into the search bar to cause the Website to search its contents.

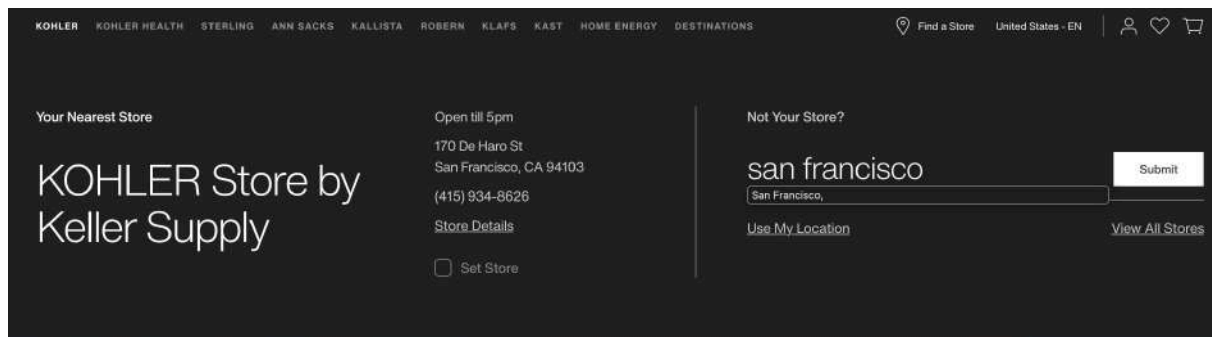


36. The other Websites also include a search bar that allow users to input search queries and search the Websites.

37. When users input the information into the search bar, they are intending to communicate with the Website the contents of the search to receive the information they are interested in.

38. Instead, the software on the Websites cause the contents of the communication entered into the search bar to be intercepted while in transit by the Third Parties.

39. The Kohler and Kallista Websites also offer a feature that allows a user to search for the nearest store or showroom. Below is an example of the search results of inputting “San Francisco” into the “Find a Store” search bar on the Kohler Website:



40. When users input the information into the “Find a Store” search bar, they are intending to communicate with the Website the contents of the search to receive the information they are interested in.

41. Instead, the software on the Websites cause the contents of the communication entered into the search bar to be intercepted while in transit by the Third Parties.

2. Facebook Cookies (Kohler, Robern, and Kallista Websites)

42. Defendant causes third party cookies to be transmitted to and from the Kohler, Robern, and Kallista Websites users’ browsers and devices to and from the facebook.com domain, even after users elect to “Reject All” cookies. This domain is associated with Meta’s digital advertising and analytics platform that collects user information via cookies to assist Meta in performing data collection, behavioral analysis, user retargeting, and analytics.² Meta serves targeted ads to web users across Meta’s ad network, which spans millions of websites and apps.

² <https://www.facebook.com/privacy/policies/cookies/>.

43. The Facebook cookies help Meta track whether users complete specific actions after interacting with an ad (e.g., clicking a link or making a purchase) and provide analytic metrics that advertisers use to measure ad campaign performance. For example, the Kohler Website causes the following type of data to be sent to Meta when the user clicks a button:



GET https://www.facebook.com/privacy_sandbox/pixel/register/r.com%2Fen&rl=&if=false&ts=1742242724339&cd[buttonFeatures]n%22%3A%22%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22s%22%3A%0%2C%22tag%22%3A%22span%22%2C%22type%22%3Anull%7DOHLER%20Kitchen%20and%20Bathroom%22%7D&sw=5120&sh=1440&v=2.

Request Header Query Body Cookies Raw Summary +

Key	Value
id	455893950331490
ev	SubscribedButtonClick
di	https%3A%2F%2Fwww.kohler.com%2Fen
rl	
if	false
ts	1742242724339
cd[buttonFeatures]	%7B"classList"%3A"gbh-hamber-menu%20icon-Hamburger"%2C"destination"%3A""%2C"id"%3A""%2C"imageUrl"%3A"%2Ficons%2Ficon-Hamburger.svg"%2C"innerText"%3A""%2C"numChildButtons"%3A0%2C"tag"%3A"span"%2C"type"%3Anull%7D
cd[buttonText]	
cd[formFeatures]	%5B%5D
cd[pageFeatures]	%7B"title"%3A"KOHLER%20Kitchen%20and%20Bathroom"%7D
sh	1440
v	2.9.187
r	stable
ec	2
o	12318
fbp	fb.1.1742242666505.92075027844012233
ler	empty
cdi	API_unavailable
it	1742242666394
coo	false
es	automatic
tm	3
exp	k0
rqm	FGGET

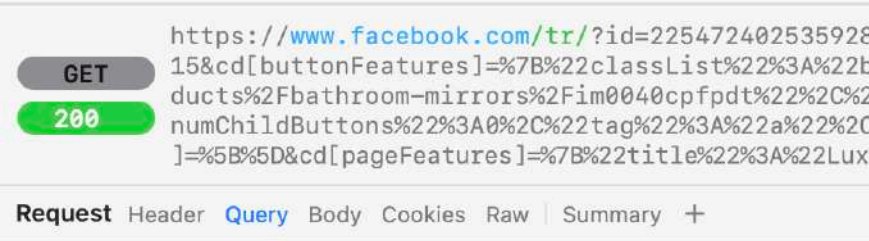
44. The “ev” parameter is an “Event.” In this case, the event is a “SubscribedButtonClick.” indicating to Facebook that the user has viewed a specific webpage on the Website.

45. The “dl” parameter is the “Document Location.” It tells Facebook the specific webpage on which the Event occurred – in this case, <https://www.kohler.com/en>.

46. The “ts” parameter corresponds to a “Timestamp,” and tells Facebook the exact time—down to the millisecond—at which the user viewed the page.

47. The “fbp” parameter is the Facebook Browser ID, and is used to track the user’s activity across the Internet.

48. Similar data is sent when users utilize the Robern Website:



Request	Header	Query	Body	Cookies	Raw	Summary	+
Key	Value						
id	225472402535928						
ev	SubscribedButtonClick						
dl	https://www.robern.com						
rl							
if	false						
ts	1761842080115						
cd[buttonFeatures]	%7B"classList"%3A"btn%20btn-primary%20btn-md"%2C"destination"%3A"%3A"%2Fwww.robern.com%2Fproducts%2Fbathroom-mirrors%2Fim0040cpfpdt"%2C"id"%3A""%2C"imageA""%2C"innerText"%3A"VIEW%20PRODUCT"%2C"numChildButtons"%3A0%2C"tag"%3A"a"%2C"type"%3Anull%me"%3A""%7D						
cd[buttonText]	VIEW%20PRODUCT						
cd[formFeatures]	%5B%5D						
cd[pageFeatures]	%7B"title"%3A"Luxury%20Bathroom%20Vanities%2Cabinets%2C%20Mirrors%20%26%20Lighting%20%7Robern"%7D						

cd[parameters]	%5B%7B"extractorID"%3A"1145643120097037"%2(D"%3A%7B"%40context"%3A"http%3A%2F%2Fsche"%2C"%40type"%3A"Product"%2C"offers"%3A%7B"urrency"%3A"USD"%7D%7D%7D%2C%7B"extractorID"%3A"1183925296076507"%2C"jsonLD"%3A%7B"%40co"%3A"http%3A%2F%2Fschema.org"%2C"%40type"%2C"%2C"offers"%3A%7B"priceCurrency"%3A"USD"%7D%7D%2C%7B"extractorID"%3A"86125233602490C"jsonLD"%3A%7B"%40context"%3A"http%3A%2F%2Fema.org"%2C"%40type"%3A"Product"%2C"offers"%7D%7D%7D%2C%7B"extractorID"%3A"16140297884"%2C"jsonLD"%3A%7B"%40context"%3A"http%3A%2F%2Fschema.org"%2C"%40type"%3A"Product"%2C"%3A%7B%7D%7D%7D%5D
sw	2560
sh	1440
v	2.9.239
r	stable
ec	5
o	12318
fbp	fb.1.1761842045567.710218612110424139
cs_est	true
ler	empty
cdl	API_unavailable
pmd[description]	Roborn%20offers%20luxury%20medicine%20cabinet%20vanities%2C%20lighting%2C%20and%20access%20that%20transform%20everyday%20routines%20intn%20experience.
pmd[contents]	%5B%5D
plt	473.1999999284744
it	1761842045551
coo	false
es	automatic
tm	3
expv2[0]	pl0
expv2[1]	el3
expv2[2]	bc1
rqm	GET

49. Similar data is sent when users utilize the Kallista Website:

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

https://www.facebook.com/privacy_sandbox/pixel/register
ista.com%2F&rl=&if=false&ts=1761842588186&cd[buttonFeat
C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22inner
2type%22%3A%22button%22%2C%22name%22%3A%22%22%2C%22valu
B%22title%22%3A%22Luxurious%20Design%20Solutions%20for%20f

GET 200

Request Header Query Body Cookies Raw Summary +

Key	Value
ts	1761842588186
cd[buttonFeatures]	%7B"classList"%3A"accordion- button"%2C"destination"%3A""%2C"id"%3A""%2C"imageUr l"%3A""%2C"innerText"%3A"BATH"%2C"numChildButtons" %3A0%2C"tag"%3A"button"%2C"type"%3A"button"%2C"n ame"%3A""%2C"value"%3A""%7D
cd[buttonText]	BATH
cd[formFeatures]	%5B%5D
cd[pageFeatures]	%7B"title"%3A"Luxurious%20Design%20Solutions%20for% 20Bathroom%20%26%20Kitchen%20%7C%20Kallista"%7D
sw	2560
sh	1440
v	2.9.239
r	stable
ec	2
o	12318
fbp	fb.1.1761842568504.97651565170911550
ler	empty
cdl	API_unavailable
pmd[description]	KALLISTA%20offers%20luxury%20designer%20faucets%20 and%20fixtures%20in%20a%20variety%20of%20traditional %2C%20transitional%20and%20modern%20styles%20to%2 0outfit%20any%20bathroom%20or%20kitchen.
pmd[contents]	%5B%5D
plt	1864.5
it	1761842568416
coo	false
es	automatic
tm	3
expv2[0]	pl0
expv2[1]	el2
expv2[2]	bc1
rqm	FGET

25 50. Cookies are sent along with all data transmissions to Meta. For instance, the
26 following cookies were sent along with the SubscribedButtonClick event on the
27 Kohler Website:
28

1
2
3
4
5
6
7
8
9

https://www.facebook.com/privacy_sandbox/pixel/register
r.com%2Fen&rl=&if=false&ts=1742242724339&cd[buttonFeatu
n%22%3A%22%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%2
s%22%3A0%2C%22tag%22%3A%22span%22%2C%22type%22%3Anull%7
OHLER%20Kitchen%20and%20Bathroom%22%7D&sw=5120&sh=1440&v=2

GET 200

Request Header Query Body Cookies Raw Summary +

Key	Value
datr	5mbYZ1jKbXy6aDYmQeG12nLI
sb	5mbYZ56GJQ_sWb_zfkbhZwT5
c_user	100076133960803
xs	3%3ALn6HViH61md_pA%3A2%3A1742235391%3A-1%3A-1
ar_debug	1
fr	0SZZHlnSGtNtWvaUg.AWXeYJ57CnjDolyUm_bMb87pmisOPwz9 gEhpsA.Bn2Gbm..AAA.0.0.Bn2HvJ.AWUtx8VwJDQ

10 51. The same type of cookie data is sent when using the Robern Website:

11
12
13
14
15
16
17
18
19
20

https://www.facebook.com/tr/?id=225472402535928&ev=Subs
15&cd[buttonFeatures]=%7B%22classList%22%3A%22btn%20btn
ducts%2Fbathroom-mirrors%2Fim0040cpfpdt%22%2C%22id%22%3
numChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%
]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22Luxury%20Bat

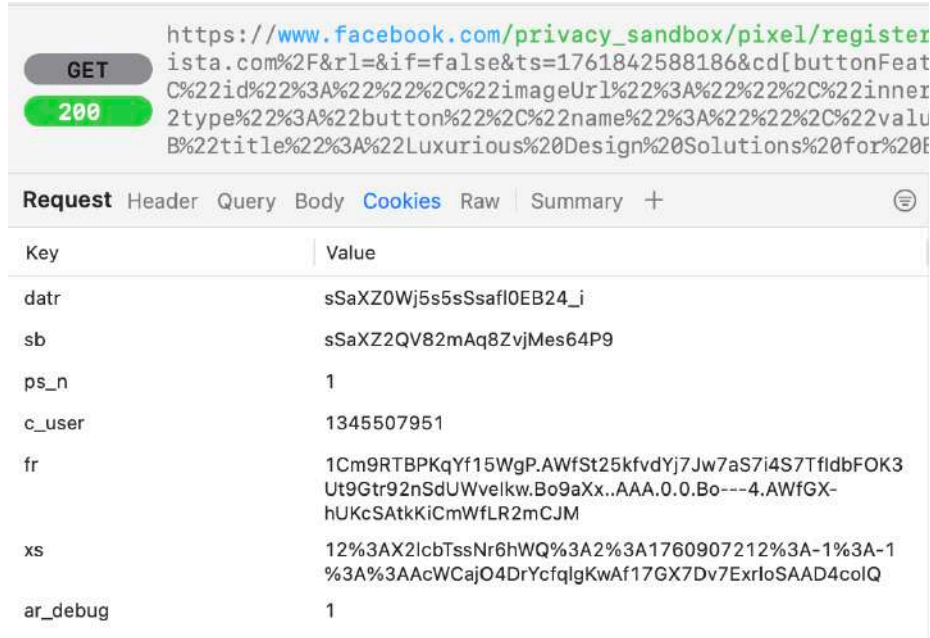
GET 200

Request Header Query Body Cookies Raw Summary +

Key	Value
datr	sSaXZ0Wj5s5sSsafI0EB24_i
sb	sSaXZ2QV82mAq8ZvjMes64P9
ps_n	1
c_user	1345507951
fr	1Cm9RTBPKqYf15WgP.AWfSt25kfvdYj7Jw7aS7i4S7TfldbFOK3 Ut9Gtr92nSdUWvelkw.Bo9aXx...AAA.0.0.Bo---4.AWfGX- hUKcSAtkKiCmWfLR2mCJM
xs	12%3AX2lcbTssNr6hWQ%3A2%3A1760907212%3A-1%3A-1 %3A%3AAcWCajO4DrYcfqlgKwAf17GX7Dv7ExrloSAAD4colQ
ar_debug	1

21 52. The same type of cookie data is sent when using the Kallista Website:

22
23
24
25
26
27
28



https://www.facebook.com/privacy_sandbox/pixel/register

GET 200

ista.com%2F&rl=&if=false&ts=1761842588186&cd[buttonFeat
C%22id%22%3A%22%22%22%22imageUrl%22%3A%22%22%22inner
2type%22%3A%22button%22%2C%22name%22%3A%22%22%22valu
B%22title%22%3A%22Luxurious%20Design%20Solutions%20for%20F

Request Header Query Body Cookies Raw Summary +

Key	Value
datr	sSaXZ0Wj5s5sSsafI0EB24_i
sb	sSaXZ2QV82mAq8ZvjMes64P9
ps_n	1
c_user	1345507951
fr	1Cm9RTBPKqYf15WgP.AWfSt25kfvdYj7Jw7aS7i4S7TfldbFOK3 Ut9Gtr92nSdUWvelkw.Bo9aXx...AAA.0.0.Bo---4.AWfGX- hUKcSAtkKiCmWfLR2mCJM
xs	12%3AX2lcbTssNr6hWQ%3A2%3A1760907212%3A-1%3A-1 %3A%3AAcWCajO4DrYcfqlgKwAf17GX7Dv7ExrIoSAAD4colQ
ar_debug	1

53. The “c_user” cookie shown above causes Facebook to identify a specific user when they are logged in to their account. The “c_user” cookie stores a user’s unique ID, which is associated with their Facebook profile. This ID enables Facebook to track user interactions on its platform and across sites that use Facebook plugins, such as adding items to a cart, clicking “Like” buttons, or engaging with comment sections. When combined with other data sent to the Facebook domain, this cookie allows Meta to track users’ browsing activities. Facebook uses this data for various purposes, such as personalizing content, enhancing ad targeting accuracy, and refining its user experience.

54. In particular, by identifying users who have shown interest in certain products or content, the Facebook cookies cause Meta’s advertising platform to enable advertisers to show relevant ads to those users when they visit other websites within Meta’s ad network.³ These cookies allow Meta to collect data on how users interact with websites, regardless of whether they have a Facebook account or are logged in.⁴

55. The Facebook cookies allow Meta to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v)

³ *Id.*; <https://allaboutcookies.org/what-data-does-facebook-collect>.

⁴ <https://allaboutcookies.org/what-data-does-facebook-collect>.

demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data (including IP addresses)—which can be used to determine whether a user is located in California.⁵

56. Meta utilizes the data collected through the Facebook cookies for its own purposes, including by using the data to tailor content and target advertisements to users. This includes practices such as (i) **Ad Targeting and Retargeting**, in which Meta uses the facebook.com cookie to track users' online behavior across different sites, building a profile based on their browsing habits, purchases, and interactions. This profile enables Facebook to deliver highly targeted ads within the Facebook ecosystem and on other sites that are part of Facebook's Audience Network; (ii) **Conversion Tracking**, in which Meta uses the facebook.com cookie to enable business partners to track specific actions users take after viewing or clicking on a Facebook ad, such as making a purchase or signing up for a newsletter; (iii) **Audience Insights and Analytics**, in which Meta uses the facebook.com cookie to provide data to businesses on user demographics, interests, and behaviors across their sites and apps; and (iv) **Cross-Device and Cross-Platform Tracking**, in which Meta uses the facebook.com cookie to support tracking users across devices and platforms, so that ads are targeted consistently regardless of the device a user is on. This ensures that advertisers can follow users across devices.

57. In addition, the software code executed when a user visits the Websites causes the consumer's browser to send "header" data to Facebook. This data includes the "user-agent," which corresponds to the device and browser that the user has used to access the Website:

user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/ 537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/ 537.36
------------	---

58. In this case, the user-agent value corresponds to Google's Chrome browser version 126, running on Windows.⁶

⁵ *Id.*

⁶ There are many tools on the web that are capable of parsing user-agent strings to determine what browser and operating system they pertain to. One such tool is located at <https://explore.whatismybrowser.com/useragents/parse>.

3. TikTok Cookies (Kohler Website)

59. Defendant also causes third party cookies to be transmitted to and from Kohler Website users' browsers and devices, even after users elect to "Reject All" cookies, to and from the analytics.tiktok.com domain. This domain is associated with TikTok for Business, a suite of tools offered by TikTok, a social media platform owned by ByteDance Ltd., known for short-form video sharing.⁷ The TikTok platform is used to create and share videos, and it utilizes cookies for various purposes including assisting brands and marketers to create, manage, and optimize ad campaigns on the platform.⁸

60. TikTok utilizes analytics.tiktok.com cookies to collect data on user interactions with websites that have integrated TikTok's tracking technologies (such as the Website). These cookies are used to "measure and improve the performance of your advertising campaigns and to personalize the user's experience (including ads) on TikTok."⁹ TikTok further explains that it uses cookies to "match events with people who engage with your content on TikTok. Matched events are used to improve measurement and optimize ad campaigns. They can also contribute to building your retargeting and engagement audiences." *Id.* These cookies cause TikTok to recognize and track users across different sessions and domains (i.e., cross-site tracking) and to collect and synchronize user data to observe and evaluate TikTok user behavior.

61. These cookies cause TikTok to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, including *email addresses and phone numbers*; (v) demographic information, (vi) interests and

⁷ See Our advertising and measurement cookies (available at <https://business.safety.google/adscookies/>).

⁸ See, e.g., TikTok for Business (<https://ads.tiktok.com/business/en-US/products/ads>; and <https://ads.tiktok.com/business/en-US/products/measurement>); TikTok Business Help Center; Using Cookies with TikTok Pixel (available at <https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en>).

⁹ TikTok Business Help Center; Using Cookies with TikTok Pixel (available at <https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en>).

preferences, (vii) shopping behaviors, (viii) device information, (ix) session information, (x) user identifiers, and (xi) geolocation data in the form of the IP address.¹⁰

62. For example, the TikTok software code that Defendant causes to be stored on and executed by the Kohler Website user's device causes the following data to be sent to TikTok's domain, at <https://analytics.tiktok.com/api/v2/pixel/act>:

```

1  {
2    "_inspection": {
3      "ppf": [
4        {
5          "d": 800,
6          "f": [
7            {
8              "d": 0,
9              "id": 25
10           }
11         ],
12         "id": 11
13       }
14     ],
15     "action": "Metadata",
16     "auto_collected_properties": {
17       "content_data": {
18         "json_ld": "[{ \"@context\": \"https://schema.org\",
19           \"@type\": \"Organization\", \"name\": \"Kohler\",
20           \"url\": \"https://www.kohler.com\", \"logo\": \"https://www.kohler.com/_next/static/media/BLOK_LOGO.00edf835.svg\",
21           \"description\": \"Discover our collection of KOHLER faucets, showers, sinks, toilets, bidets and more. Get design inspiration for your next kitchen or bath project at https://Kohler.com.\", \"sameAs\": [\"https://www.facebook.com/Kohler/\", \"https://x.com/Kohler\", \"https://en.wikipedia.org/wiki/Kohler_Co.\"], \"contactPoint\": {
22             \"@type\": \"ContactPoint\", \"ContactType\": \"Customer Support\", \"telephone\": \"1-800-456-4537\",
23             \"mainEntityOfPage\": { \"@type\": \"WebSite\", \"name\": \"Kohler\", \"url\": \"https://www.kohler.com\",
24             \"potentialAction\": { \"@type\": \"SearchAction\", \"target\": { \"@type\": \"EntryPoint\",
25             \"urlTemplate\": \"https://www.kohler.com/en/search/?keyword={search_term_string}\", \"query-input\": \"required name=search_term_string\" } } } } ] } ]\",

```

¹⁰ *Id.*; see also TikTok for Business: Enhance Data Postback with the TikTok Pixel (<https://ads.tiktok.com/help/article/enhance-data-postback-with-the-tiktok-pixel?lang=en>); TikTok for Business: Advanced Matching for Web (available at <https://ads.tiktok.com/help/article/advanced-matching-web?redirected=1>); TikTok for Business: About TikTok Pixel (available at <https://ads.tiktok.com/help/article/tiktok-pixel?lang=en>).

```

20      "meta": "{\\"title\\":\\"KOHLER Kitchen and Bathroom\\",
    \\"meta:description\\":\\"Discover our collection of KOHLER
    faucets, showers, sinks, toilets, bidets and more. Get
    design inspiration for your next kitchen or bath project.
    \\"}",
21      "microdata": "[]",
22      "open_graph": "{\\"og:title\\":\\"KOHLER Kitchen and
    Bathroom\\",\\"og:type\\":\\"website\\",
    \\"og:site_name\\":\\"kohler\\",\\"og:url\\":\\"https://www.
    kohler.com/en/\",\\"og:image\\":[\\"https://www.kohler.com/
    _next/static/media/BLOK_LOGO.00edf835.svg\\",\\"https://www.
    kohler.com/_next/static/media/BLOK_LOGO.00edf835.svg\\"],
    \\"og:description\\":\\"Discover our collection of KOHLER
    faucets, showers, sinks, toilets, bidets and more. Get
    design inspiration for your next kitchen or bath project.
    \\"}",
23    },
24    "page_trigger": "Click"
25  },
26  "context": {
27    "ad": {
28      "jsb_status": 2,
29      "sdk_env": "external"
30    },
31    "device": {
32      "platform": "pc"
33    },
34    "index": 0,
35    "library": {
36      "name": "pixel.js",
37      "version": "2.2.0"
38    },
39    "page": {
40      "load_progress": "2",
41      "referrer": "",
42      "url": "https://www.kohler.com/en"
43    },
44    "pageview_id":
    "e3dc9061-036c-11f0-b0be-b83fd2fa8b9e-0yJ--.0.
    0::e3dc6d29-036c-11f0-b0be-b83fd2fa8b9e",
45    "pixel": {
46      "code": "C09E2F50Q3DFKFN94EP0",
47      "codes": "C09E2F50Q3DFKFN94EP0",
48      "runtime": "1"
49    },
50    "session_id":
    "e3dc9061-036c-11f0-b0be-b83fd2fa8b9e::jBoKuX2tveuKsK9uKQb
    z",
51    "user": {
52      "anonymous_id": "01JPJW2P1SA3KQ1990TAWF6AHK_.tt.1"
53    },
54    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
    AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0
    Safari/537.36",
55    "variation_id": "test_2_single_track"
56  },
57  "event_id": "",
58  "is_onsite": false,
59  "message_id": "messageId-1742242683697-1480865829504",

```

```

60     "properties": {},
61     "signal_diagnostic_labels": {
62         "hashed_email": {
63             "label": "missing"
64         },
65         "hashed_phone": {
66             "label": "missing"
67         },
68         "raw_auto_email": {
69             "label": "missing"
70         },
71         "raw_auto_phone": {
72             "label": "missing"
73         },
74         "raw_email": {
75             "label": "missing"
76         },
77         "raw_phone": {
78             "label": "missing"
79         }
80     },
81     "timestamp": "2025-03-17T20:18:03.697Z"
82 }

```

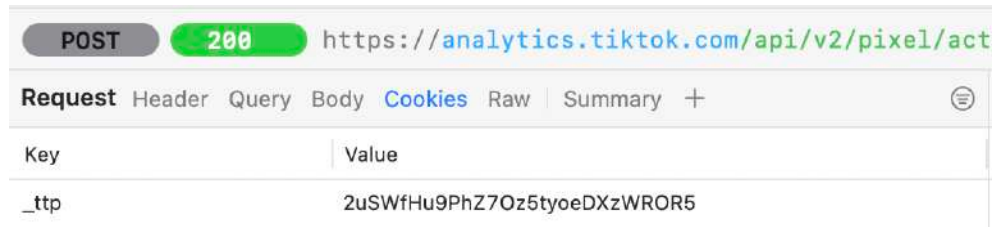
63. The data includes the “session_id,” which is a unique identifier generated by TikTok to track a user’s activity. This allows TikTok to correlate the user’s behavior from a browsing session, including page views and conversions, to a particular user to enhance advertising measurement, attribution, and targeting.¹¹

64. The data further indicates, among other things, that the user has viewed the page on the Defendant’s website at the url <https://www.kohler.com>, and that the title of that page is “KOHLER Kitchen and Bathroom.”

65. The data also discloses that the user is using a PC device, and that the user’s user-agent is “Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36.” As described above, this discloses to TikTok extensive information about the user’s device and browser.

66. Along with this data, the TikTok software code that Defendant causes to be stored on and executed by the user’s device causes the “_ttp” cookie to be sent to TikTok’s domain:

¹¹ See, e.g., How to get TikTok session id? (available at <https://gbtimes.com/how-to-get-tiktok-session-id/>).



67. According to TikTok’s documentation, the “_ttp” cookie is one of the company’s advertising cookies, the purpose of which is “[t]o measure and improve the performance of your advertising campaigns and to personalize the user’s experience (including ads) on TikTok.”¹²

68. Further, along with all of this data, the TikTok software code that Defendant causes to be stored on and executed by the user’s device causes the user’s “user-agent” information to be sent to TikTok as part of the header:

Key	Value
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36

69. Finally, the data sent to TikTok includes the user’s IP address—which can be used to determine a user’s geolocation, including whether they are located in California.

70. By collecting this user data, TikTok performs user behavior tracking, i.e., monitoring user actions like page views, clicks, and interactions to understand user engagement; advertising optimization, i.e., gathering data to enhance the relevance and effectiveness of TikTok advertising campaigns; and performance measurement (i.e., assessing the success of marketing efforts by analyze user responses to ads and content).¹³

71. Further, TikTok’s Automatic Advanced Matching feature functions as follows: “When a visitor lands on your website and inputs customer information during registration, sign-

¹² See TikTok for Business: Using Cookies with TikTok Pixel (available at <https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en>).

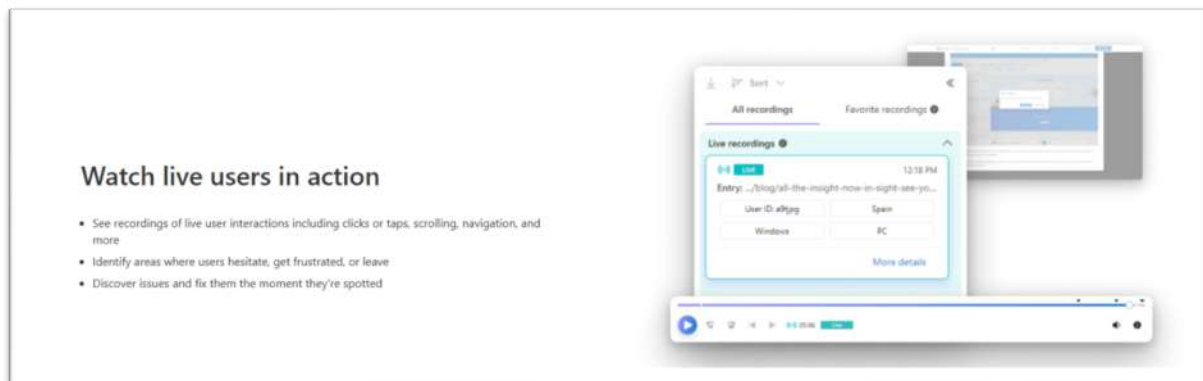
¹³ See TikTok for Business: Using Cookies with TikTok Pixel (available at <https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en>).

in, contact, or checkout on a website where you installed your pixel, Automatic Advanced Matching will capture information from those fields. ...TikTok will use hashed information to link event information to people on TikTok. Tiktok may use matched events to better attribute events to TikTok ads, optimize advertisers' future campaigns, and depending on advertisers' and users' settings, TikTok may also add people to advertisers' retargeting or engagement audiences."¹⁴

4. Microsoft Clarity Cookies (Kohler Website)

72. Defendant also causes third-party cookies to be transmitted to and from Kohler Website users' browsers and devices, even after users click or select the "Reject All" button, to and from the clarity.ms domain. This domain is associated with Clarity, Microsoft's "cutting-edge behavioral analytics tool that helps you understand user interaction with your website or app".¹⁵ Clarity is a Microsoft Advertising tool, which "crucial for successful marketing."¹⁶ "Clarity's tracking code ... uses a cookie to obtain user session data."¹⁷

73. Clarity allows Defendant to "watch live users in action" via "recordings of live user interactions" on the website, including a user's "clicks or taps, scrolling, navigation, and more."¹⁸ Indeed, Clarity boasts that it "tracks all visitor clicks and scrolls on mobile, desktop,



¹⁴ TikTok for Business: How to set up Automatic Advanced Matching (available at <https://ads.tiktok.com/help/article/how-to-set-up-automatic-advanced-matching?lang=en>).

¹⁵ <https://learn.microsoft.com/en-us/clarity/setup-and-installation/about-clarity>.

¹⁶ <https://about.ads.microsoft.com/en/blog/post/october-2021/introducing-microsoft-clarity-insights-for-microsoft-advertising>.

¹⁷ <https://learn.microsoft.com/en-us/clarity/setup-and-installation/cookie-consent>.

¹⁸ <https://clarity.microsoft.com/session-recordings>.

and tablet[.]” These “session recordings” track each and every consumer’s individual actions on the website.¹⁹

74. Further, Clarity permits Defendant to aggregate individual users’ session recordings into “heatmaps” for Defendant’s financial gain. Heatmaps are “visualization tool[s]” aimed at “aggregat[ing] information about how users interact with the website.”²⁰ This allows Defendant to “See at a glance which areas on [web site owner’s] page drive the most engagement,” a crucial element to increasing advertising revenue.²¹ Clarity also permits Defendant to “track a specific subset of users,” including tracking metrics like what browser users visited from, what type of device, the date, and more. Clarity even permits the use of specific “Clarity user ID[s]” which permits Clarity to track users across their devices, and identify when the same user visits multiple times to the website.²² Businesses use Clarity to “make data-driven decisions” to “improve overall conversion rates” of clicks, engagement, or sales.²³ Microsoft notes in a Clarity case study that Clarity cookies permitted businesses to see a “substantial increase” in “purchases.”²⁴ In one instance, “following just five days after implementing Clarity, the [business] saw an uplift of 19% in conversion rate.”²⁵ Businesses consider Clarity a “must-have tool for any business serious about optimizing their website and increasing online revenue.”²⁶

¹⁹ <https://clarity.microsoft.com/session-recordings>.

²⁰ <https://learn.microsoft.com/en-us/clarity/heatmaps/heatmaps-overview>.

²¹ <https://clarity.microsoft.com/heatmaps>.

²² <https://clarity.microsoft.com/insights>; <https://learn.microsoft.com/en-us/clarity/setup-and-installation/identify-api>.

²³ <https://clarity.microsoft.com/case-studies/ecommerce-boost/#:~:text=Using%20Clarity&text=By%20analyzing%20user%20sessions%20and,and%20improve%20overall%20conversion%20rates>.

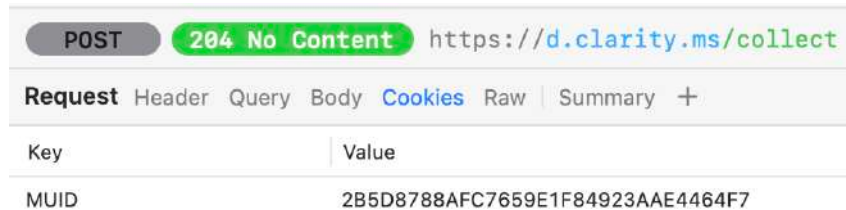
²⁴ *Id.*

²⁵ *Id.*, emphasis in original.

²⁶ <https://clarity.microsoft.com/case-studies/ecommerce-boost/#:~:text=Using%20Clarity&text=By%20analyzing%20user%20sessions%20and,and%20improve%20overall%20conversion%20rates>.

75. Microsoft collects data from Clarity,²⁷ which “Microsoft retains . . . for as long as necessary[.]”²⁸ Clarity cookies allow Microsoft to obtain and store at least the following user data: (i) user identifier; (ii) website interactions; (iii) interests and preferences; (iv) shopping behavior; (v) device information; (vi) demographic data; (vii) geolocation data; (viii) referring URL; and (ix) session information.²⁹

76. The type of cookie data sent to Microsoft along with the screen recording data is as follows:



Key	Value
MUID	2B5D8788AFC7659E1F84923AAE4464F7

77. Microsoft’s documentation confirms that the “MUID” cookie “[i]dentifies unique web browsers visiting Microsoft sites” and is “used for advertising, site analytics, and other operational purposes.”³⁰

D. The Private Communications Collected are Valuable.

78. As part of its regular course of business, Defendant targets California consumers by causing the Third Parties to extract, collect, maintain, distribute, and exploit for Defendant’s and the Third Parties’ profit, all of the Private Communications transferred by the cookies which Defendant causes to be placed on the devices of Plaintiff and other California users of the Websites without their knowledge or consent. Defendant knew the location of consumers like Plaintiff and the Class members either prior to or shortly after causing the Third Parties to use cookies on their devices.

79. The Private Communications that the Third Parties track and collect by way of the cookies on the Websites are valuable to Defendant as well as the Third Parties. Defendant

²⁷ <https://www.microsoft.com/en-us/privacy/privacystatement>.

²⁸ *Id.*

²⁹ <https://learn.microsoft.com/en-us/clarity/setup-and-installation/clarity-data>.

³⁰ <https://learn.microsoft.com/en-us/clarity/setup-and-installation/clarity-cookies>

1 can use the data to create and analyze the performance of marketing campaigns, website design,
2 product placement, and target specific users or groups of users for advertisements. For instance,
3 if Defendant wanted to market certain of its plumbing products, such as certain of its bathroom
4 fixtures, to consumers in California, Defendant could use the data collected by the Third Parties
5 to monitor the location of users who visit webpages related to specific products, then advertise
6 similar products to those particular users when they visit other webpages. The third-party cookies
7 also enable Defendant to target online advertisements to users when they visit *other* websites,
8 even those completely unrelated to Defendant and its products.

9 80. Data about users' browsing history enables Defendant to spot patterns in users'
10 behavior on the Websites and their interests in, among other things, Defendant's plumbing
11 products. On a broader scale, it enables Defendant to gain an understanding of trends happening
12 across its brands and across the construction materials market. All of this helps Defendant further
13 monetize its Websites and maximize revenue by collecting and analyzing user data.

14 81. The value of the Private Communications tracked and collected by the Third
15 Parties using cookies on the Websites can be quantified. Legal scholars observe that "[p]ersonal
16 information is an important currency in the new millennium."³¹ Indeed, "[t]he monetary value
17 of personal data is large and still growing, and corporate America is moving quickly to profit
18 from the trend." *Id.* "Companies view this information as a corporate asset and have invested
19 heavily in software that facilitates the collection of consumer information." *Id.*

20 82. Numerous empirical studies quantify the appropriate value measure for personal
21 data. Generally, the value of personal data is measured as either the consumer's willingness to
22 accept compensation to sell her data or the consumer's willingness to pay to protect her
23 information.

24 83. Through its false representations and aiding, agreeing with, employing,
25 permitting, or otherwise enabling the Third Parties to track users' Private Communications on
26 the Websites using third-party cookies, Defendant is unjustly enriching itself at the cost of
27

28 ³¹ See Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 Harv. L. Rev. 2055, 2056–57 (2004).

1 consumer privacy and choice, when the consumer could otherwise have the ability to choose if
2 and how they would monetize their data.

3 **PLAINTIFF'S EXPERIENCES**

4 84. Plaintiff Beltran visited the Kohler Website to seek and obtain information about
5 Kohler's products, while located in California, on one or more occasions during the last four
6 years.

7 85. Plaintiff Beltran's visits to the Kohler Website were consistent with a typical
8 Website user's visits seeking information about Defendant's products. Specifically, Plaintiff
9 Beltran is not a consumer advocate, a "tester," or a compliance auditor that visited the Kohler
10 Website to test or evaluate Defendant's privacy practices.

11 86. When Plaintiff Beltran visited the Kohler Website, the Website immediately
12 detected that he was a visitor in California and presented him with Defendant's popup cookie
13 consent banner, which provided the option to select the "Reject All" button. Plaintiff Beltran
14 viewed Defendant's representation on the popup cookie consent banner that, "Cookies may be
15 used on this site and stored on your device to enhance site navigation, analyze site usage, enable
16 troubleshooting session recording for optimized customer support resolution, and assist in our
17 marketing efforts." Plaintiff Beltran also viewed Defendant's additional representation that,
18 rather than clicking or selecting the "Accept All Cookies" button to accept all such cookies, users
19 could instead click or select the "Reject All" button to reject "All" cookies.

20 87. Consistent with his typical practice in rejecting or otherwise declining the
21 placement or use of cookies and tracking technologies, Plaintiff Beltran selected and clicked the
22 "Reject All" button. Plaintiff Beltran believed that selecting the "Reject All" button on the popup
23 cookie consent banner found on the Kohler Website would allow him to opt out of, decline,
24 and/or reject "All" cookies and other tracking technologies (inclusive of those cookies that cause
25 the disclosure of tracking data to third-party advertising networks and analytics services for the
26 purpose of enabling usage analytics, session recording, and Defendant's marketing efforts).

27 88. In selecting the "Reject All" button, Plaintiff Beltran gave Defendant notice that
28 he did not consent to the use or placement of cookies and tracking technologies while browsing

1 the Kohler Website. Further, Plaintiff Beltran specifically rejected, based on Defendant's
2 representations, those cookies used to "enhance site navigation, analyze site usage, enable
3 troubleshooting session recording...and assist in [Defendant's] marketing efforts" and share
4 information with third parties. In reliance on these representations and promises, only then did
5 Plaintiff Beltran continue browsing the Kohler Website.

6 89. Even before the popup cookie consent banner appeared on the screen, Defendant
7 nonetheless caused cookies and tracking technologies, including those used for advertising,
8 analytics, and session recording, to be placed on Plaintiff Beltran's device and/or transmitted to
9 the Third Parties along with user data, without Plaintiff Beltran's knowledge. Accordingly, the
10 popup cookie consent banner's representation to Plaintiff Beltran that he could reject the use
11 and/or placement of all cookies and tracking technologies while he browsed the Kohler Website
12 was false. Contrary to what Defendant made Plaintiff Beltran believe, he did not have a choice
13 about whether third-party cookies would be placed on his device and/or transmitted to the Third
14 Parties along with his user data; rather, Defendant had already caused that to happen.

15 90. Then, as Plaintiff Beltran continued to browse the Kohler Website in reliance on
16 the promises Defendant made in the cookie consent banner, and despite Plaintiff Beltran's clear
17 rejection of the use and/or placement of "All" such cookies and tracking technologies, Defendant
18 nonetheless continued to cause the placement and/or transmission of cookies along with user
19 data, including those involved in providing advertising, analytics, and session recording services
20 or functions from the Third Parties on his device. In doing so, Defendant permitted the Third
21 Parties to track and collect Plaintiff Beltran's Private Communications as he browsed the Kohler
22 Website.

23 91. Defendant's representations that consumers could "Reject All" cookies while
24 Plaintiff Beltran and users browsed the Kohler Website, or at least those involved in providing
25 advertising, analytics, and session recording services, were untrue. Had Plaintiff Beltran known
26 this fact, he would not have used the Kohler Website. Moreover, Plaintiff Beltran reviewed the
27 popup cookie consent banner prior to using the Kohler Website. Had Defendant disclosed that it
28 would continue to cause cookies and tracking technologies to be stored on consumers' devices

1 even after they choose to “Reject All” cookies, Plaintiff Beltran would have noticed it and would
2 not have used the Kohler Website or, at a minimum, he would have interacted with the Website
3 differently.

4 92. Plaintiff Beltran continues to desire to browse content featured on the Websites.
5 Plaintiff Beltran would like to browse websites that do not misrepresent that users can reject all
6 cookies and tracking technologies. If the Websites were programmed to honor users’ requests to
7 reject all cookies and tracking technologies, Plaintiff Beltran would likely browse the Websites
8 again in the future, but will not do so until then. Plaintiff Beltran regularly visits websites that
9 feature content similar to that of the Websites. Because Plaintiff Beltran does not know how the
10 Websites are programmed, which can change over time, and because he does not have the
11 technical knowledge necessary to test whether the Websites honor users’ requests to reject all
12 cookies and tracking technologies, Plaintiff Beltran will be unable to rely on Defendant’s
13 representations when browsing the Websites in the future absent an injunction that prohibits
14 Defendant from making misrepresentations on the Websites. The only way to determine what
15 network traffic is sent to third parties when visiting a website is to use a specialized tool such as
16 Chrome Developer Tools. As the name suggests, such tools are designed for use by “developers”
17 (i.e., software developers), whose specialized training enables them to analyze the data
18 underlying the HTTP traffic to determine what data, if any, is being sent to whom. Plaintiff
19 Beltran is not a software developer and has not received training with respect to HTTP network
20 calls.

21 **CLASS ALLEGATIONS**

22 93. Plaintiff brings this Class Action Complaint on behalf of himself and a proposed
23 class of similarly situated persons, pursuant to Rules 23(b)(2) and (b)(3) of the Federal Rules of
24 Civil Procedure. Plaintiff seeks to represent the following group of similarly situated persons,
25 defined as follows:
26
27
28

1 102. To plead an invasion of privacy claim, Plaintiff must show an invasion of (i) a
2 legally protected privacy interest; (ii) where Plaintiff had a reasonable expectation of privacy in
3 the circumstances; and (iii) conduct by Defendant constituting a serious invasion of privacy.

4 103. Defendant has intruded upon the following legally protected privacy interests of
5 Plaintiff and Class members: (i) the California Invasion of Privacy Act, as alleged herein; (ii) the
6 California Constitution, which guarantees Californians the right to privacy; (iii) the California
7 Wiretap Acts as alleged herein; (iv) Cal. Penal Code § 484(a), which prohibits the knowing theft
8 or defrauding of property “by any false or fraudulent representation or pretense,” and
9 (v) Plaintiff’s and Class members’ Fourth Amendment right to privacy.

10 104. Plaintiff and Class members had a reasonable expectation of privacy under the
11 circumstances, as Defendant affirmatively promised users they could “Reject All” cookies and
12 tracking technologies before proceeding to browse the Websites. Plaintiff and other Class
13 members directed their electronic devices to access the Websites and, when presented with the
14 popup cookies consent banner on the Websites, Plaintiff and Class members rejected “All”
15 cookies and reasonably expected that their rejection of “All” cookies and tracking technologies
16 would be honored. That is, they reasonably believed that Defendant would not permit the Third
17 Parties to store and send cookies and/or use other such tracking technologies on their devices
18 while they browsed the Websites. Plaintiff and Class members also reasonably expected that, if
19 they rejected “All” such cookies and/or tracking technologies, Defendant would not permit the
20 Third Parties to track and collect Plaintiff’s and Class members’ Private Communications,
21 including their browsing history, visit history, website interactions, user input data, demographic
22 information, interests and preferences, shopping behaviors, device information, referring URLs,
23 session information, user identifiers, and/or geolocation data, on the Websites.

24 105. Such information is “personal information” under California law, which defines
25 personal information as including “Internet or other electronic network activity information,”
26 such as “browsing history, search history, and information regarding a consumer’s interaction
27 with an internet website, application, or advertisement.” Cal. Civ. Code § 1798.140.
28

106. Defendant, in violation of Plaintiff's and other Class members' reasonable expectation of privacy and without their consent, permits the Third Parties to use cookies and other tracking technologies to collect, track, and compile users' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—including whether a user is located in California. The data that Defendant allowed third parties to collect enables the Third Parties to (and they in fact do), *inter alia*, create consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics; create audience segments based on shared traits (such as Millennials, Californians, tech enthusiasts, etc.); and perform targeted advertising and marketing analytics. Further, the Third Parties share user data and/or the user profiles to unknown parties to further their financial gain. The consumer profiles are and can be used to further invade Plaintiff's and users' privacy, by allowing third parties to learn intimate details of their lives, and target them for advertising and other purposes, as described herein, thereby harming them through the abrogation of their autonomy and their ability to control dissemination and use of information about them.

107. Defendant's actions constituted a serious invasion of privacy in that it invaded a zone of privacy protected by the Fourth Amendment (i.e., one's personal communications), and violated criminal laws on wiretapping and invasion of privacy. These acts constitute an egregious breach of social norms that is highly offensive.

108. Defendant's intrusion into Plaintiff's privacy was also highly offensive to a reasonable person.

109. Defendant lacked a legitimate business interest in causing the placement and/or transmission of third-party cookies along with user data that allowed the Third Parties to track, intercept, receive, and collect Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, without their consent.

110. Plaintiff and Class members have been damaged by Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

111. Plaintiff and Class members seek appropriate relief for that injury, including but not limited to, damages that will compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiff's and Class members' privacy.

112. Plaintiff and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and Class members and made in conscious disregard of Plaintiff's and Class members' rights and Plaintiff's and Class members' rejection of the Websites' use of "All" cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Second Cause of Action: Intrusion Upon Seclusion

113. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

114. To assert a claim for intrusion upon seclusion, Plaintiff must plead (i) that Defendant intentionally intruded into a place, conversation, or matter as to which Plaintiff had a reasonable expectation of privacy; and (ii) that the intrusion was highly offensive to a reasonable person.

115. By permitting third-party cookies to be stored on consumers' devices without consent, which caused the Third Parties to track and collect Plaintiff's and Class members' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, in violation of Defendant's representations otherwise in the popup cookie consent banner, Defendant intentionally intruded upon the solitude or seclusion of users of the Websites. Defendant effectively placed the Third Parties in the middle of communications to which they were not invited, welcomed, or authorized.

116. The Third Parties' tracking and collecting of Plaintiff's and Class member's Private Communications on the Websites using third-party cookies that Defendant caused to be

1 stored on users' devices—and to be transmitted to Third Parties—was not authorized by Plaintiff
2 and Class members, and, in fact, those users of the Websites specifically chose to “Reject All”
3 cookies.

4 117. Plaintiff and the Class members had an objectively reasonable expectation of
5 privacy surrounding their Private Communications on the Websites based on Defendant's
6 promise that users could “Reject All” cookies, as well as state criminal and civil laws designed
7 to protect individual privacy.

8 118. Defendant's intentional intrusion into Plaintiff's and other users' Private
9 Communications would be highly offensive to a reasonable person given that Defendant
10 represented that users of the Websites could “Reject All” cookies when, in fact, Defendant
11 caused such third-party cookies to be stored on consumers' devices and browsers, and to be
12 transmitted to third parties, even when consumers rejected all such cookies. Indeed, Plaintiff and
13 Class members reasonably expected, based on Defendant's false representations, that when they
14 rejected all cookies and tracking technologies, Defendant would not cause such third-party
15 cookies to be stored on their devices or permit the Third Parties to obtain their Private
16 Communications on the Websites, including their browsing history, visit history, website
17 interactions, user input data, demographic information, interests and preferences, shopping
18 behaviors, device information, referring URLs, session information, user identifiers, and/or
19 geolocation data—including whether a user is located in California.

20 119. Defendant's conduct was intentional and intruded on Plaintiff's and Website
21 users' Private Communications on the Websites.

22 120. Plaintiff and Class members have been damaged by Defendant's invasion of their
23 privacy and are entitled to just compensation, including monetary damages.

24 121. Plaintiff and Class members seek appropriate relief for that injury, including but
25 not limited to, damages that will compensate them for the harm to their privacy interests as well
26 as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiff's and
27 Class members' privacy.
28

122. Plaintiff and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and Class members and made in conscious disregard of Plaintiff's and Class members' rights and Plaintiff's and Class members' rejection of the Websites' use of "All" cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Third Cause of Action: Wiretapping in Violation of the California Invasion of Privacy Act (California Penal Code § 631)

123. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

124. California Penal Code § 631(a) provides, in pertinent part:

"Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars"

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

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

While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and *its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device*.

As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements.

Ribas, 38 Cal. 3d at 360-61 (emphasis supplied; internal citations omitted).

127. CIPA § 631(a) imposes liability for “distinct and mutually independent patterns of conduct.” *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under § 631(a), Plaintiff need only establish that Defendant, “by means of any machine, instrument, contrivance, or in any other manner,” did **any** of the following:

[i] Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system;

[ii] Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state;

[iii] Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained

Cal. Penal Code § 631(a).

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

129. Defendant is a “person” within the meaning of California Penal Code § 631.

130. Section 631(a) is not limited to phone lines, but also applies to “new technologies” such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new technologies” and must be construed broadly to effectuate its remedial purpose of protecting privacy); *see also Bradley v. Google, Inc.*, 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006) (CIPA governs “electronic communications”); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) (“Though written in terms of wiretapping, Section 631(a) applies to Internet communications.”).

131. The Third Parties’ cookies—as well as the software code of the Third Parties responsible for placing the cookies and transmitting data from user devices to the Third Parties—constitute “machine[s], instrument[s], or contrivance[s]” under the CIPA (and, even if they do

not, Defendant’s deliberate and purposeful scheme that facilitated the interceptions falls under the broad statutory catch-all category of “any other manner”).

132. Each of the Third Parties is a “separate legal entity that offers [a] ‘software-as-a-service’ and not merely a passive device.” *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Further, the Third Parties had the capability to use the wiretapped information for their own purposes and, as alleged above, they did in fact use the wiretapped information for their own business purposes. Accordingly, the Third Parties were third parties to any communication between Plaintiff and Class members, on the one hand, and Defendant, on the other. *Id.* at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

133. Under § 631(a), Defendant must show it had the consent of all parties to a communication.

134. At all relevant times, the Websites caused Plaintiff’s and Class members’ browsers to store the Third Parties’ cookies and to transmit those cookies alongside Private Communications—including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—to the Third Parties without Plaintiff’s and Class members’ consent. By configuring the Websites in this manner, Defendant willfully aided, agreed with, employed, permitted, or otherwise caused the Third Parties to wiretap Plaintiff and Class members using the Third Parties’ cookies and to accomplish the wrongful conduct alleged herein.

135. At all relevant times, by their cookies and corresponding software code, the Third Parties willfully and without the consent of all parties to the communication, or in any unauthorized manner, read, attempted to read, and/or learned the contents or meaning of electronic communications of Plaintiff and Class members, on the one hand, and Defendant, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

1 136. The Private Communications of Plaintiff and Class members, on the one hand,
2 and Defendant, on the other, that the Third Parties automatically intercepted directly
3 communicates the Website user's affirmative decisions, actions, choices, preferences, and
4 activities, which constitute the "contents" of electronic communications, including their
5 browsing history, visit history, website interactions, user input data, demographic information,
6 interests and preferences, shopping behaviors, device information, referring URLs, session
7 information, user identifiers, and/or geolocation data—including whether a user is located in
8 California.

9 137. At all relevant times, the Third Parties used or attempted to use the Private
10 Communications automatically intercepted by their cookie tracking technologies for their own
11 purposes.

12 138. Plaintiff and Class members did not provide their prior consent to the Third
13 Parties' intentional access, interception, reading, learning, recording, collection, and usage of
14 Plaintiff's and Class members' electronic communications. Nor did Plaintiff and Class members
15 provide their prior consent to Defendant aiding, agreeing with, employing, permitting, or
16 otherwise enabling the Third Parties' conduct. On the contrary, Plaintiff and Class members
17 expressly declined to allow Third Parties' cookies and tracking technologies to access, intercept,
18 read, learn, record, collect, and use Plaintiff's and Class members' electronic communications
19 by choosing to reject "All" cookies in the consent banner.

20 139. The wiretapping of Plaintiff and Class members occurred in California, where
21 Plaintiff and Class members accessed the Websites and where the Third Parties—as caused by
22 Defendant—routed Plaintiff's and Class members' electronic communications to Third Parties'
23 servers. Among other things, the cookies, as well as the software code responsible for placing
24 the cookies and transmitting them and other Private Communications to the Third Parties,
25 resided on Plaintiff's California-located device. In particular, the user's California-based device,
26 after downloading the software code from the Third Parties' servers, (i) stored the code onto the
27 user's disk; (ii) converted the code into machine-executable format; and (iii) executed the code,
28 causing the transmission of data (including cookie data) to and from the Third Parties.

140. Plaintiff and Class members have suffered loss by reason of these violations, including, but not limited to, (i) violation of their right to privacy, (ii) loss of value in their Private Communications, (iii) damage to and loss of Plaintiff's and Class members' property right to control the dissemination and use of their Private Communications, and (iv) loss of their Private Communications to the Third Parties with no consent.

141. Pursuant to California Penal Code § 637.2, Plaintiff and Class members have been injured by the violations of California Penal Code § 631, and each seeks statutory damages of the greater of \$5,000, or three times the amount of actual damages, for each of Defendant's violations of CIPA § 631(a), as well as injunctive relief.

142. Unless enjoined, Defendant will continue to commit the illegal acts alleged herein including, but not limited to, permitting third parties to access, intercept, read, learn, record, collect, and use Plaintiff's and Class members' electronic Private Communications with Defendant. Plaintiff, Class members, and the general public continue to be at risk because Plaintiff, Class members, and the general public frequently use the internet to search for information and content related to plumbing fixtures and related home improvement products. Plaintiff, Class members, and the general public continue to desire to use the internet for that purpose. Plaintiff, Class members, and the general public have no practical way to know if their request to reject "All" cookies and tracking technologies will be honored and/or whether Defendant will permit third parties to access, intercept, read, learn, record, collect, and use Plaintiff's and Class members' electronic Private Communications with Defendant. Further, Defendant has already permitted the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiff's and Class members' electronic Private Communications with Defendant and will continue to do so unless and until enjoined.

Fourth Cause of Action: Use of a Pen Register in Violation of the California Invasion of Privacy Act (California Penal Code § 638.51)

143. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

144. The California Invasion of Privacy Act, codified at Cal. Penal Code §§ 630 to 638, includes the following statement of purpose:

1 The Legislature hereby declares that advances in science and technology have led
2 to the development of new devices and techniques for the purpose of
3 eavesdropping upon private communications and that the invasion of privacy
4 resulting from the continual and increasing use of such devices and techniques
has created a serious threat to the free exercise of personal liberties and cannot be
tolerated in a free and civilized society.

5 145. California Penal Code Section 638.51(a) proscribes any “person” from
6 “install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court
7 order.”

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

12 147. The Third Parties’ cookies and the corresponding software code installed by
13 Defendant on its Websites are each “pen registers” because they are “device[s] or process[es]”
14 that “capture[d]” the “routing, addressing, or signaling information”—including, the IP address
15 and user-agent information—from the electronic communications transmitted by Plaintiff’s and
16 the Class’s computers or devices. Cal. Penal Code § 638.50(b).

17 148. At all relevant times, Defendant caused the Third Parties’ cookies and the
18 corresponding software code—which are pen registers—to be placed on Plaintiff’s and Class
19 members’ browsers and devices, and/or to be used to transmit Plaintiff’s and Class members’ IP
20 address and user-agent information. *See Greenley v. Kochava*, 2023 WL 4833466, at *15-16
21 (S.D. Cal. July 27, 2023); *Shah v. Fandom, Inc.*, 2024 U.S. Dist. LEXIS 193032, at *5-11 (N.D.
22 Cal. Oct. 21, 2024).

23 149. Some of the information collected by the Third Parties’ cookies and the
24 corresponding software, including IP addresses and user-agent information, does not constitute
25 the content of Plaintiff’s and the Class members’ electronic communications with the Websites.
26 *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1008 (9th Cir. 2014). (“IP addresses constitute
27 addressing information and do not necessarily reveal any more about the underlying contents of
28 communication...” (cleaned up).

1 150. Plaintiff and Class members did not provide their prior consent to Defendant's
2 use of third-party cookies and the corresponding software. On the contrary, Plaintiff and the
3 Class members informed Defendant that they did not consent to the Websites' use of third-party
4 cookies by clicking or selecting the "Reject All" button in the cookie consent banner.

5 151. Defendant did not obtain a court order to install or use the third-party cookies and
6 corresponding software to track and collect Plaintiff's and Class member's IP addresses and
7 user-agent information.

8 152. As a direct and proximate result of Defendant's conduct, Plaintiff and Class
9 members suffered losses and were damaged in an amount to be determined at trial.

10 153. Pursuant to Penal Code § 637.2(a)(1), Plaintiff and Class members are also
11 entitled to statutory damages of \$5,000 for each of Defendant's violations of § 638.51(a).

12 **Fifth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation**

13 154. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

14 155. Defendant fraudulently and deceptively informed Plaintiff and Class members
15 that they could "Reject All" cookies.

16 156. However, despite Defendant's representations otherwise, Defendant caused third-
17 party cookies and software code to be stored on consumers' devices, and to be transmitted to the
18 Third Parties alongside Private Communications, even after users clicked or selected the "Reject
19 All" cookies button in the popup cookie consent banner. These cookies and corresponding
20 software code allowed the Third Parties to access, intercept, read, learn, record, collect, and use
21 Plaintiff's and Class members' Private Communications, even when consumers had previously
22 chosen to "Reject All" cookies.

23 157. These misrepresentations and omissions were known exclusively to, and actively
24 concealed by Defendant, not reasonably known to Plaintiff and Class members, and material at
25 the time they were made. Defendant knew, or should have known, how the Websites functioned,
26 including the Third Party's resources it installed on the Websites and the third-party cookies in
27 use on the Websites, through testing the Websites, evaluating its performance metrics by means
28 of its accounts with the Third Parties, or otherwise, and knew, or should have known, that the

1 Websites' programming allowed the third-party cookies to be placed on Website users'—
2 including Plaintiff's—browsers and devices and/or transmitted to the Third Parties along with
3 users' Private Communications even after users attempted to "Reject All" cookies, which
4 Defendant promised its users they could do. Defendant's misrepresentations and omissions
5 concerned material facts that were essential to the analysis undertaken by Plaintiff and Class
6 members as to whether to use the Websites. In misleading Plaintiff and Class members and not
7 so informing them, Defendant breached its duty to Plaintiff and Class members. Defendant also
8 gained financially from, and as a result of, its breach.

9 158. Plaintiff and Class members relied to their detriment on Defendant's
10 misrepresentations and fraudulent omissions.

11 159. Plaintiff and Class members have suffered an injury-in-fact, including the loss of
12 money and/or property, as a result of Defendant's unfair, deceptive, and/or unlawful practices,
13 including the unauthorized interception of their Private Communications, including their
14 browsing history, visit history, website interactions, user input data, demographic information,
15 interests and preferences, shopping behaviors, device information, referring URLs, session
16 information, user identifiers, and/or geolocation data, which have value as demonstrated by the
17 use and sale of consumers' browsing activity, as alleged above. Plaintiff and Class members
18 have also suffered harm in the form of diminution of the value of their private and personally
19 identifiable information and communications.

20 160. Defendant's actions caused damage to and loss of Plaintiff's and Class members'
21 property right to control the dissemination and use of their personal information and
22 communications.

23 161. Defendant's representation that consumers could "Reject All" cookies (including
24 those used to "enhance site navigation, analyze site usage, enable troubleshooting session
25 recording...and assist in [Defendant's] marketing efforts") if they clicked or selected the "Reject
26 All" button was untrue. Again, had Plaintiff and Class members known these facts, they would
27 not have used the Websites. Moreover, Plaintiff and Class members reviewed the popup cookie
28 consent banner prior to their interactions with the Websites. Had Defendant disclosed that it

1 caused third-party cookies to be stored on the devices of visitors of the Websites that are related
2 to advertising, analytics, and session recording, and/or share information with third parties even
3 after they choose to reject “All” such cookies, Plaintiff and Class members would have noticed
4 it and would not have interacted with the Websites.

5 162. By and through such fraud, deceit, misrepresentations and/or omissions,
6 Defendant intended to induce Plaintiff and Class members to alter their positions to their
7 detriment. Specifically, Defendant fraudulently and deceptively induced Plaintiff and Class
8 members to, without limitation, use the Websites under the mistaken belief that Defendant would
9 not permit third parties to obtain users’ Private Communications when consumers chose to
10 “Reject All” cookies. As a result, Plaintiff and the Class provided more personal data than they
11 would have otherwise.

12 163. Plaintiff and Class members justifiably and reasonably relied on Defendant’s
13 misrepresentations and omissions, and, accordingly, were damaged by Defendant’s conduct.

14 164. As a direct and proximate result of Defendant’s misrepresentations and/or
15 omissions, Plaintiff and Class members have suffered damages, as alleged above, and are entitled
16 to just compensation, including monetary damages.

17 165. Plaintiff and Class members seek punitive damages because Defendant’s
18 actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and
19 Class members and made in conscious disregard of Plaintiff’s and Class members’ rights and
20 Plaintiff’s and Class members’ rejection of the Websites’ use of “All” cookies. Punitive damages
21 are warranted to deter Defendant from engaging in future misconduct.

22 **PRAYER FOR RELIEF**

23 **WHEREFORE**, reserving all rights, Plaintiff, on behalf of himself and the Class
24 members, respectfully requests judgment against Defendant as follows:

25 A. Certification of the proposed Class, including appointment of Plaintiff’s counsel
26 as class counsel;

1 B. An award of compensatory damages, including statutory damages where
2 available, to Plaintiff and Class members against Defendant for all damages sustained as a result
3 of Defendant's wrongdoing, including both pre- and post-judgment interest thereon;

4 C. An award of punitive damages;

5 D. An award of nominal damages;

6 E. An order for full restitution;

7 F. An order requiring Defendant to disgorge revenues and profits wrongfully
8 obtained;

9 G. An order temporarily and permanently enjoining Defendant from continuing the
10 unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

11 H. For reasonable attorneys' fees and the costs of suit incurred; and

12 I. For such further relief as may be just and proper.

13 Dated: November 8, 2025

14 **GUTRIDE SAFIER LLP**

15 /s/Seth A. Safier/s/

Seth A. Safier (State Bar No. 197427)

seth@gutridesafier.com

16 Marie A. McCrary (State Bar No. 262670)

marie@gutridesafier.com

17 Todd Kennedy (State Bar No. 250267)

todd@gutridesafier.com

18 100 Pine Street, Suite 1250

San Francisco, CA 94111

19 Telephone: (415) 639-9090

20 Facsimile: (415) 449-6469

21 *Attorneys for Plaintiff*

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

Martin Beltran

(b) County of Residence of First Listed Plaintiff San Francisco, CA
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Seth Safier, SBN 197427, Gutride Safier LLP, 100 Pine

DEFENDANTS

Kohler Co.

County of Residence of First Listed Defendant Sheybogan, WI
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

☐ 1 U.S. Government Plaintiff

☐ 2 U.S. Government Defendant

☐ 3 Federal Question
(U.S. Government Not a Party)

☒ 4 Diversity
(Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

	PTF	DEF
Citizen of This State	<input checked="" type="checkbox"/> 1	<input type="checkbox"/> 1
Citizen of Another State	<input type="checkbox"/> 2	<input type="checkbox"/> 2
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3

IV. NATURE OF SUIT (Place an "X" in One Box Only)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
110 Insurance	PERSONAL INJURY	625 Drug Related Seizure of Property 21 USC § 881	422 Appeal 28 USC § 158	375 False Claims Act
120 Marine	310 Airplane	690 Other	423 Withdrawal 28 USC § 157	376 Qui Tam (31 USC § 3729(a))
130 Miller Act	315 Airplane Product Liability	LABOR	PROPERTY RIGHTS	400 State Reapportionment
140 Negotiable Instrument	320 Assault, Libel & Slander	710 Fair Labor Standards Act	820 Copyrights	410 Antitrust
150 Recovery of Overpayment of Veteran's Benefits	330 Federal Employers' Liability	720 Labor/Management Relations	830 Patent	430 Banks and Banking
151 Medicare Act	340 Marine	740 Railway Labor Act	835 Patent—Abbreviated New Drug Application	450 Commerce
152 Recovery of Defaulted Student Loans (Excludes Veterans)	345 Marine Product Liability	751 Family and Medical Leave Act	840 Trademark	460 Deportation
153 Recovery of Overpayment of Veteran's Benefits	350 Motor Vehicle	790 Other Labor Litigation	880 Defend Trade Secrets Act of 2016	470 Racketeer Influenced & Corrupt Organizations
160 Stockholders' Suits	355 Motor Vehicle Product Liability	791 Employee Retirement Income Security Act	SOCIAL SECURITY	480 Consumer Credit
190 Other Contract	360 Other Personal Injury	IMMIGRATION	861 HIA (1395ff)	485 Telephone Consumer Protection Act
195 Contract Product Liability	362 Personal Injury -Medical Malpractice	462 Naturalization Application	862 Black Lung (923)	490 Cable/Sat TV
196 Franchise	CIVIL RIGHTS	465 Other Immigration Actions	863 DIWC/DIWW (405(g))	850 Securities/Commodities/Exchange
REAL PROPERTY	PRISONER PETITIONS		864 SSID Title XVI	890 Other Statutory Actions
210 Land Condemnation	HABEAS CORPUS		865 RSI (405(g))	891 Agricultural Acts
220 Foreclosure	440 Other Civil Rights		FEDERAL TAX SUITS	893 Environmental Matters
230 Rent Lease & Ejectment	441 Voting		870 Taxes (U.S. Plaintiff or Defendant)	895 Freedom of Information Act
240 Torts to Land	442 Employment		871 IRS—Third Party 26 USC § 7609	896 Arbitration
245 Tort Product Liability	443 Housing/Accommodations			899 Administrative Procedure Act/Review or Appeal of Agency Decision
290 All Other Real Property	445 Amer. w/Disabilities—Employment			950 Constitutionality of State Statutes
	446 Amer. w/Disabilities—Other			
	448 Education			
	OTHER			
	540 Mandamus & Other			
	550 Civil Rights			
	555 Prison Condition			
	560 Civil Detainee—Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

☒ 1 Original Proceeding

☐ 2 Removed from State Court

☐ 3 Remanded from Appellate Court

☐ 4 Reinstated or Reopened

☐ 5 Transferred from Another District (specify)

☐ 6 Multidistrict Litigation—Transfer

☐ 8 Multidistrict Litigation—Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):

28 USC s 1332

Brief description of cause:

violation of consumer protection statutes; fraud; privacy violations

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P.

DEMAND \$

CHECK YES only if demanded in complaint: JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S), IF ANY (See instructions):

JUDGE

DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only)

☒ SAN FRANCISCO/OAKLAND

☐ SAN JOSE

☐ EUREKA-MCKINLEYVILLE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I. a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the “defendant” is the location of the tract of land involved.)
- c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section “(see attachment).”
- II. Jurisdiction.** The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an “X” in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
 - (1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.
 - (2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an “X” in this box.
 - (3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 - (4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an “X” in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.
- V. Origin.** Place an “X” in one of the six boxes.
 - (1) Original Proceedings. Cases originating in the United States district courts.
 - (2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.
 - (3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 - (4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 - (5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 - (6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.
 - (8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket. Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an “X” in this box if you are filing a class action under Federal Rule of Civil Procedure 23. Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction. Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.
- IX. Divisional Assignment.** If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: “the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated.”

Date and Attorney Signature. Date and sign the civil cover sheet.