STEVEN M. NATHAN, SBN 153250
HAUSFELD LLP
33 Whitehall Street
Fourteenth Floor
New York, NY 10034
Tel: (646) 357-1100
Fax: (212) 202-4322
snathan@hausfeld.com

Attorneys for Plaintiff
(additional counsel on signature page)

IN THE UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF CALIFORNIA

ANNE LIGHTOLLER, individually and on behalf of all others similarly situated,
Plaintiff,
vs.

TCF CO. LLC, d/b/a The Cheesecake Factory,
Defendant.

Case No.: '23CV0272 AJB NLS

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

COMPLAINT - CLASS ACTION

Plaintiff, Anne Lightoller ("Plaintiff"), individually and on behalf of all others similarly situated, hereby files this class action complaint against Defendant TCF Co. LLC d/b/a The Cheesecake Factory ("Defendant" or "TCF"), and in support thereof alleges the following:

INTRODUCTION

1. This is a class action brought against TCF for wiretapping the electronic communications of visitors to its website, www.thecheesecakefactory.com. TCF procures third-party vendors, such as Microsoft Corporation, to embed snippets of JavaScript computer code ("Session Replay Code") on TCF's website, which then deploys on each website visitor's internet browser for the purpose of intercepting and

recording the website visitor's electronic communications with the TCF website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time ("Website Communications"). These third-party vendors (collectively, "Session Replay Providers") create and deploy the Session Replay Code at TCF's request.

2. After intercepting and capturing the Website Communications, TCF and the Session Replay Providers use those Website Communications to recreate website visitors' entire visit to www.thecheesecakefactory.com. The Session Replay Providers create a video replay of the user's behavior on the website and provide it to TCF for analysis. TCF's procurement of the Session Replay Providers to secretly deploy the Session Replay Code results in the electronic equivalent of "looking over the shoulder" of each visitor to the TCF website for the entire duration of their website interaction.

3. TCF's conduct violates the California Invasion of Privacy Act, Cal. Penal Code § 630 *et seq*. and constitutes the torts of invasion of the privacy rights and intrusion upon seclusion of website visitors.

4. Plaintiff brings this action individually and on behalf of a class of all California citizens whose Website Communications were intercepted through TCF's procurement and use of Session Replay Code embedded on www.thecheesecakefactory.com, as well as its subpages, and seeks all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, and attorneys' fees and costs.

PARTIES

5. Plaintiff Anne Lightoller is a citizen of the State of California, and at all times relevant to this action, resided and was domiciled in California. Plaintiff is a citizen of California.

6. Defendant TCF Co. LLC is a limited liability company organized under the laws of Nevada, and its principal place of business is located in Nevada. Defendant is a citizen of Nevada.

JURISDICTION AND VENUE

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

8. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in California. Further, Defendant purposefully directed its activities to California, consummated transactions in California and purposefully availed itself of the privilege of conducting activities in California thereby invoking the benefits and protections of California law. Specifically, Plaintiff, while in California, accessed and viewed the www.thecheesecakefactory.com website and placed and paid for orders for take-out and/or delivery of food from TCF's brick and mortar stores located in California. Further, Plaintiff paid for the delivery and/or take-out orders through the www.thecheesecakefactory.com website.

9. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of California while they were located within California. At all relevant times, Defendant knew that its practices would directly result in the collection of information from California citizens while those citizens browse and place delivery and/or take-out orders on, www.thecheesecakefactory.com. Defendant chose to avail itself of the business opportunities of marketing and selling its goods and services in California and collecting real-time data from website visit sessions initiated by Plaintiff while located in California, and the claims alleged herein arise from those activities.

10. TCF also knows that many users visit and interact with TCF's website while they are physically present in California. Both desktop and mobile versions of TCF's website allow a user to search for nearby restaurants by providing the user's "current location," as furnished by the location-determining tools of the device the user is using or by the user's IP address (*i.e.*, without requiring the user to manually input an address). Through its website, www.thecheesecakefactory.com, TCF represents that it has 38 brick and mortar restaurants in California.[1] Each restaurant location takes delivery and take-out orders via the website in addition to allowing viewing of their menu.

11. Users' employment of automatic location services in this way means that TCF is continuously made aware that its website is being visited by people located in California, and that such website visitors are being wiretapped in violation of California statutory and common law.

12. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value.

13. The "world's most valuable resource is no longer oil, but data."[2]

14. Earlier this year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business's website, applications, and emails), behavioral data (*i.e.*, customers' purchase histories and product usage

[1] See locations.thecheesecakefactory.com.

[2] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data.

information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.[3] This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.[4]

15. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[5]

16. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[6] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[7]

17. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[8]

[3] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, Business News Daily (Aug. 5, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

[4] *Id.*

[5] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.

[6] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

[7] *Id.* at 25.

[8] *Id.*

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites.

18. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that "a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected."[9]

19. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.[10] As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[11]

20. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

21. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[12]

[9] Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/.

[10] *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html.

[11] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, The Information Society, 38:4, 257, 258 (2022).

[12] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

22. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[13]

23. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[14]

C. How Session Replay Code Works.

24. Session Replay Code, such as that implemented on www.thecheesecakefactory.com, enables website operators to record, save, and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with insights into the user experience by recording website visitors "as they click, scroll, type or navigate across different web pages."[15]

25. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website operator, or has not finished

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

[14] Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

[15] Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/.

submitting the data to the website operator.[16] As a result, website visitors "aren't just sharing data with the [web]site they're on . . . but also with an analytics service that may be watching over their shoulder."[17]

26. Session Replay Code works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the occurrence of actions the user takes. When a website delivers Session Replay Code to a user's browser, the browser will follow the code's instructions by sending responses in the form of "event" data to a designated third-party server. Typically, the server receiving the event data is controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

27. The types of events captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user's navigation and interaction through the website. In order to permit a reconstruction of a user's visit accurately, the Session Replay Code must be capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are typically accumulated and transmitted in blocks periodically throughout the user's website session, rather than after the user's visit to the website is completely finished.

28. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the Session Replay Provider.

29. Once the events from a user session have been recorded by a Session Replay Code, a website operator can view a visual reenactment of the user's visit

[16] *Id.*

[17] Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0.

through the Session Replay Provider, usually in the form of a video, meaning "[u]nlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions."[18]

30. Because most Session Replay Codes will by default indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.[19]

31. Most alarming, Session Replay Code may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a "submit" or "enter" button on the website, the Session Replay Code may nevertheless cause the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the Session Replay Provider.

32. Session Replay Code does not necessarily anonymize user sessions, either.

33. First, if a user's entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

34. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

[18] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

[19] *Id.*

35. Third, some Session Replay Providers explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.[20]

36. Session Replay Providers often create "fingerprints" that are unique to a particular user's combination of computer and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, is collected across all sites that the Session Replay Provider monitors.

37. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user's other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

38. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.[21] Indeed, "[t]he more copies of sensitive information that exist, the broader the attack surface, and when data is being collected [ ] it may not be stored properly or have standard protections" increasing "the overall risk that data will someday publicly leak or be breached."[22]

[20] *Id.*; *see also* *FS.identify – Identifying users*, FullStory, https://help.fullstory.com/hc/en-us/articles/360020828113, (last visited Sep. 8, 2022).

[21] Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720.

[22] Lily Hay Newman, *Covert 'Replay Sessions' Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/.

39. The privacy concerns arising from Session Replay Code are not theoretical or imagined. The CEO and founder of LOKKER, a provider of data privacy and compliance solutions has said "[consumers] should be concerned" about the use of Session Replay Code because "they won't know these tools are operating 'behind the scenes' of their site visit" and "even if the company disclosed that they are using these tools, consumers wouldn't likely be able to opt-out and still use the site."[23]

40. Indeed, the news is replete with examples of the dangers of Session Replay Code. For example, in 2019, the App Analyst, a mobile expert who writes about his analyses of popular apps, found that Air Canada's iPhone app wasn't properly masking the session replays they were sent, exposing unencrypted credit card data and password information.[24] This discovery was made just weeks after Air Canada said its app had a data breach, exposing 20,000 profiles.[25]

41. Further, multiple companies have removed Session Replay Code from their websites after it was discovered the Session Replay Code captured highly sensitive information. For instance, in 2017, Walgreens stopped sharing data with a Session Replay Provider after it was discovered that the Session Replay provider gained access to website visitors' sensitive information.[26] Indeed, despite Walgreens' extensive use of manual redactions for displayed and inputted data, the Session Replay Provider still gained access to full names of website visitors, their medical conditions, and their prescriptions.[27]

[23] Mark Huffner, *Is 'session replay software' a privacy threat or just improving your web experience*, Consumer Affairs (Oct. 25, 2022), https://www.consumeraffairs.com/news/is-session-replay-software-a-privacy-threat-or-just-improving-your-web-experience-102522.html.

[24] Zach Whittaker, *Many Popular iPhone Apps Secretly Record Your Screen Without Asking*, TechCrunch (Feb. 6, 2019), https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots/.

[25] *Id.*

[26] Nitasha Tiku, *The Dark Side of 'Replay Sessions' That Record Your Every Move Online*, WIRED (Nov. 16, 2017), https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/.

[27] Englehardt, *supra* note 17.

42. Following the Walgreens incident, Bonobos, a men's clothing retailer, announced that it was eliminating data sharing with a Session Replay Provider after it was discovered that the Session Replay Provider captured credit card details, including the cardholder's name and billing address, and the card's number, expiration, and security code from the Bonobos' website.[28]

43. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from the app store.[29] In announcing this decision, Apple stated: "Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity."[30]

D. TCF Secretly Wiretaps its Website Visitors' Electronic Communications.

44. TCF operates the website www.thecheesecakefactory.com, as well as all of its subpages. The Cheesecake Factory is a restaurant that operates over 300 locations across the United States and Canada, providing in-house dining, take-out and delivery services.

45. However, unbeknownst to the millions of individuals perusing TCF's menu and products online, and those purchasing The Cheesecake Factory's products for delivery or take-out, TCF intentionally procures and embeds various Session Replay Codes from Session Replay Providers on its website to track and analyze website user interactions with www.thecheesecakefactory.com and its subpages.

46. One such Session Replay Provider that TCF procures is Microsoft.

[28] Tiku, *supra* note 25.

[29] Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), https://techcrunch.com/2019/02/07/apple-glassbox-apps/.

[30] *Id.*

47. Microsoft is the owner and operator of a Session Replay Code titled Clarity, which provides basic information about website user sessions, interactions, and engagement, and breaks down users by device type, county, and other dimensions.[31]

48. Clarity captures a user's interactions with a website, logging every website user's mouse movements and clicks, scrolling window resizing, user inputs, and more.[32] Indeed, Clarity organizes the information it captures into over 30 different categories including: the date a user visited the website, the device the user accessed the website on, the type of browser the user accessed the website on, the operating system of the device used to access the website, the country where the user accessed the website from, a user's mouse movements, a user's screen swipes, text inputted by the user on the website, and how far down a webpage a user scrolls.[33] Clarity even provides a specific user ID to each website visitor so their website use and interactions can be monitored over time. [34]

49. Similar to other Session Replay Code, the information collected and recorded by Clarity can then be used to play back a user's journey through a website, showing how they interacted with site navigation, calls to action, search features, and other on-page elements.[35] Put differently, the information Clarity captures can be translated into a simulation video of how a user interacts with a website.

50. Clarity also uses the information captured to create detailed heat-maps of a website that provide information about which elements of a website have high user

[31] Jono Alderson, *An Introduction to Microsoft Clarity*, Yoast, https://yoast.com/introduction-microsoft-clarity/#h-what-is-microsoft-clarity, (last visited Sep. 8, 2022).

[32] *Clarity Data Collection*, Microsoft, https://docs.microsoft.com/en-us/clarity/clarity-data, (last visited Aug. 24, 2022).

[33] *Filters Overview*, Microsoft (Jul. 26, 2022), https://docs.microsoft.com/en-us/clarity/clarity-filters.

[34] *Id.*

[35] Roger Montti, *Microsoft Clarity Analytics: Everything You Need to Know*, SEJ (Jan. 19, 2022), https://www.searchenginejournal.com/microsoft-clarity-analytics-overview/419311/#close.

engagement, how far website users scrolled on the website, and the total clicks within a given area on the website. [36]

51. Clarity offers websites three standard approaches when it comes to masking sensitive information collected from a user's interactions with a website—strict (all text entered by a user is purportedly masked), balanced (sensitive text entered into certain specifically pre-coded fields, such as passwords, and credit card information, is masked), and relaxed (no text entered by a user is masked).[37] When Clarity is set to "relaxed," whatever information a user enters into the field on a website can be previewed in session recordings.[38] Additionally, Clarity enables websites to select specific elements and content to mask or unmask, customizing the standard masking approaches.[39]

52. However, even when a website operator selects the "strict" and "balanced" settings, Clarity is nevertheless capable of collecting text entered by users, including text containing sensitive information.

53. As such, Clarity collects highly personal information and substantive communications that can be tied to directly to a website user's identity as it monitors, records, and collects a website user's every move.

54. Once Clarity's JavaScript is installed on a website, Clarity begins collecting website users' interactions within two hours of installation.[40] For website users who visit a website after Clarity has been installed, the wiretapping commences immediately on the visitor's web browser when the visitor loads the website in their browser.

[36] Haley Walden, *What is Microsoft Clarity? (& How Can it Improve SEO?)*, Elegant Themes (Jun. 12, 2022), https://www.elegantthemes.com/blog/wordpress/microsoft-clarity-improve-seo.

[37] *Microsoft Clarity, An Essential Part of Customer Experience Optimization*, TechAir (Aug. 17, 2022), https://privacy.microsoft.com/en-US/privacystatement.

[38] *Id.*

[39] *Masking Content*, Microsoft (Jul. 18, 2022), https://docs.microsoft.com/en-us/clarity/clarity-masking.

[40] *Frequently Asked Questions*, Microsoft, https://docs.microsoft.com/en-us/clarity/faq, (last visited Aug. 24, 2022).

55. Data collected by Clarity is then stored in the Microsoft Azure cloud service and Microsoft has access to that information. [41]

56. TCF's procurement and use of Microsoft Clarity's Session Replay Code, and procurement and use of other Session Replay Codes through various Session Replay Providers, is a wiretap in violation California statutory and common law.

E. Plaintiff's and Class Members' Experience.

57. Plaintiff has visited www.thecheesecakefactory.com and certain of its subpages on her computer and/or smartphone while in California prior to the filing of this action. She visited the website to order food, check the menu and/or to get directions to the restaurant. Plaintiff further utilized the online payment system for said orders. Plaintiff completed these transactions with TCF within the State of California.

58. While visiting TCF's website, Plaintiff fell victim to Defendant's unlawful monitoring, recording, and collection of Plaintiff's Website Communications with www.thecheesecakefactory.com.

59. Unknown to Plaintiff, TCF procures and embeds Session Replay Code on its website.

60. During a visit by Plaintiff to www.thecheesecakefactory.com and its subpages, Plaintiff browsed the menu and different product offerings. Plaintiff communicated with TCF's website by using her mouse to hover and click on certain links and items.

61. Even though Plaintiff did not always order food on her visits to TCF's website, whenever she did visit TCF's website, the Session Replay Code instantaneously captured her Website Communications throughout her visit. Indeed, through TCF's procurement of Session Replay Code, Plaintiff's Website Communications were automatically and secretly intercepted while using TCF's website.

[41] *Id.*

62. Further, without her consent, TCF procured Session Replay Providers to obtain certain information about her device, browser, and create a unique ID and profile for her.

63. The Session Replay Codes operate in the same manner for all putative Class members.

64. Like Plaintiff, each Class member visited www.thecheesecakefactory.com and its subpages with Session Replay Code embedded in it, and those Session Replay Codes intercepted the Class members' Website Communications with www.thecheesecakefactory.com by sending hyper-frequent logs of those communications to Session Replay Providers.

65. Even if TCF masks certain elements when it configures the settings of the Session Replay Code embedded on its website, any operational iteration of the Session Replay Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

66. For example, even with heightened masking enabled, Session Replay Providers will still learn through the intercepted data exactly which pages a user navigates to, how the user moves through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

F. Plaintiff and Class Members Did Not Consent to the Interception of Their Website Communications.

67. Plaintiff and Class members did not provide prior consent to TCF's interception of their Website Communications, nor could they, as the interception begins *immediately* upon arriving at www.thecheesecakefactory.com.

68. As the 2017 study recognized, the extent of data collected by Session Replay Code "far exceeds user expectations [1]; text typed into forms is collected before the user submits the form, and precise mouse movements are saved, all without any visual indication to the user."[42]

[42] Englehardt, *supra* note 17.

69. TCF does not ask website visitors, including Plaintiff and Class members, for prior consent before wiretapping their Website Communications. Indeed, Plaintiff and Class members have no idea upon arriving at the Website that TCF is using Session Replay Code to monitor, collect, and record their Website Communications because the Session Replay Code is seamlessly incorporated and embedded into TCF's Website.

70. Further, while TCF maintains a "Privacy Policy," the Privacy Policy is insufficient for Plaintiff and Class members to furnish prior consent. First, because the wiretapping begins the moment a website user visits www.thecheesecakefactory.com, Plaintiff and Class members had no opportunity to review the Privacy Policy before they were wiretapped and therefore provide insufficient and subsequent consent after the wiretapping has already occurred.

71. Moreover, a reasonable person would not be on notice of the terms of TCF's Privacy Policy by way of normal interaction with the website. TCF's Privacy Policy is contained on the homepage of www.thecheesecakefactory.com, buried at the very bottom of the website in non-contrasting font that is unobtrusive and easy to overlook. As such a reasonable person could browse TCF's website without ever being on notice of the purported Privacy Policy.

CLASS ACTION ALLEGATIONS

72. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

> All natural persons in California whose Website Communications were captured through the use of Session Replay Code embedded in www.thecheesecakefactory.com.

73. Excluded from the Class are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the Class, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

74. **Numerosity:** The members of the Class are so numerous that individual joinder of all Class members is impracticable. The precise number of Class members and their identities may be obtained from the books and records of TCF or the Session Replay Providers.

75. **Commonality:** This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to: (a) whether Defendant procures Session Replay Providers to intercept TCF's website visitors' Website Communications; (b) whether TCF intentionally discloses the intercepted Website Communications of its website users; (c) whether Defendant acquires the contents of website users' Website Communications without their consent; (d) whether Defendant's conduct violates the California Invasion of Privacy Act, Cal. Penal Code §630 *et seq.* and/or whether that conduct constitutes a tortious invasion of privacy and/or intrusion on seclusion (e) whether Plaintiff and the Class members are entitled to equitable relief; and (f) whether Plaintiff and the Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

76. **Typicality:** Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiff and each member of the Class had their communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiff and the members of the Class typical of one another.

77. **Adequacy of Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members

of the Class, and they have the resources to do so. Neither Plaintiff nor her counsel have any interest adverse to the interests of the other members of the Class.

78. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

79. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant intercepted Plaintiff's and Class members' Website Communications, then Plaintiff and each Class member suffered damages by that conduct.

80. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class members may be readily identified through TCF's books and records or the Session Replay Providers' books and records.

COUNT I

VIOLATION OF CALIFORNIA INVASION OF PRIVACY ACT

81. Plaintiff incorporates the above allegations by reference as if fully set forth herein and brings this count individually and on behalf of the Class.

82. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630-638. The Act contains the following statement of purpose:

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

83. California Penal Code § 631(a) accordingly 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 ($2,500).

84. At all relevant times, TCF's business practice of injecting Session Replay Code allowed it to access, intercept, learn the contents of and collect Plaintiff and Class members' personally identifiable information and other data.

85. Plaintiff, and each Class Member, visited and/or interacted with the TCF website while in California.

86. Plaintiff and Class members did not consent to any of TCF's actions in intercepting, reading, and learning the contents of their communications

87. TCF's conduct was intentional in that it purposefully installed code which allows it to eavesdrop and learn the content of its users' communications and other browsing activities that would otherwise be unavailable to TCF without engaging in this practice. TCF directly participated in the interception, reading, and/or learning of the contents of the communications between Plaintiff, Class members and California-based web entities.

88. The information TCF intercepts while Plaintiff and Class members are using its website includes personally identifiable information and other highly specific information and communications, including, without limitation, every button, keystroke and link a user taps, whether the user has taken any screenshots, text entries

(including passwords and credit card information), and how much time a user spent on the website.

89. Plaintiff and Class members have suffered loss by reason of these violations, including but not limited to, violation of the right to privacy. Unless restrained and enjoined, TCF will continue to commit such acts.

90. As a result of the above violations and pursuant to CIPA section 637.2, TCF is liable to Plaintiff and Class members for the greater of treble actual damages related to their loss of privacy in an amount to be determined at trial or for statutory damages in the amount of $5,000 per violation. Section 637.2 provides "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiffs has suffered, or be threatened with, actual damages."

91. Plaintiff further requests, as provided under CIPA, reasonable attorneys' fees and costs of suit, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury sufficient to prevent or deter the same or similar conduct by TCF.

<u>COUNT II</u>

INVASION OF PRIVACY – INTRUSION UPON SECLUSION

92. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

93. California law recognizes the tort of invasion of privacy/intrusion on seclusion.

94. Plaintiff brings this claim individually and on behalf of the Class.

95. Plaintiff and Class members have an objective, reasonable expectation of privacy in their Website Communications.

96. Plaintiff and Class members did not consent to, authorize, or know about TCF's invasion/intrusion at the time it occurred. Plaintiff and Class members never agreed that TCF could collect or disclose their Website Communications.

97. Plaintiff and Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in

conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

98. TCF intentionally intrudes on Plaintiff's and Class members' private life, seclusion, or solitude, without consent.

99. TCF's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

100. Plaintiff and Class members were harmed by TCF's wrongful conduct as TCF's conduct has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

101. TCF's conduct has needlessly harmed Plaintiff and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

102. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff and Class members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiff's and Class members' property.

103. Further, TCF has improperly profited from its invasion of Plaintiff and Class members' privacy in its use of their data for its economic value.

104. As a direct and proximate result TCF's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

105. TCF's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of the other members of the proposed Class, respectfully request that the Court enter judgment in Plaintiff's and the Class's favor and against Defendant as follows:

A. Certifying the Class and appointing Plaintiff as the Class representative;

B. Appointing Plaintiff's counsel as class counsel;

C. Declaring that Defendant's past conduct was unlawful, as alleged herein;

D. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;

E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;

F. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

G. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Class, demands a trial by jury of any and all issues in this action so triable of right.

DATED: February 10, 2023

Respectfully Submitted

/s/Steven M. Nathan
Steven M. Nathan, SBN 153250
HAUSFELD LLP
33 Whitehall Street
Fourteenth Floor
New York, NY 10004
Telephone: (646) 357-1100
Email: snathan@hausfeld.com

James J. Pizzirusso, D.C. Bar No. 477604*
HAUSFELD LLP
888 16th Street N.W.
Suite 300
Washington, D.C. 20006
Telephone: (202) 540-7200
Email: jpizzirusso@hausfeld.com

Stephen B. Murray, La. Bar No. 9858*
Stephen B. Murray, Jr, La. Bar No. 23877*
Arthur M. Murray, La. Bar No. 27694*
Thomas M. Beh, La. Bar No. 24018*
THE MURRAY LAW FIRM
701 Poydras Street, Suite 4250
New Orleans, Louisiana 70139
Telephone: (504) 525-8100
Email: Tbeh@Murray-lawfirm.com

Attorneys for Plaintiff

**pro hac vice forthcoming*