John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Tel.: (858) 209-6941
jnelson@milberg.com

MaryBeth V. Gibson
(pro hac vice forthcoming)
MGibson@TheFinleyFirm.com
THE FINLEY FIRM, P.C.
3535 Piedmont Road
Building 14, Suite 230
Atlanta, Georgia 30305
T: (404) 978-6971
F: (404) 320-9978
Attorneys for Plaintiff and the Proposed Class

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

JOHN TANNER, individually and on behalf of all others similarly situated, Plaintiff, v. ACUSHNET COMPANY and ACUSHNET HOLDINGS CORP., Defendants.	Case No. _____ **COMPLAINT FOR DAMAGES FOR VIOLATIONS OF:** **1. VIOLATION OF THE FEDERAL WIRETAP ACT,** **18 U.S.C. §2510 *et. seq.*** **2. UNLAWFUL WIRETAPPING AND INTERCEPTION OF ELECTRONIC COMMUNICATION,** **Cal. Pen. Code § 630**

	3. **STATUTORY LARCENY, CAL. PEN. CODE §§ 484 and 496** 4. **INVASION OF PRIVACY – INTRUSION UPON SECLUSION** **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff John Tanner ("Plaintiff"), individually and on behalf of all others similarly situated, hereby files this class action complaint against Defendants Acushnet Company and Acushnet Holdings Corp. ("Defendants" or "Acushnet"), and in support thereof alleges the following:

JURISDICTION AND VENUE

1. 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 Defendants.

2. This Court has personal jurisdiction over Defendants because a substantial part of the events and conduct giving rise to Plaintiff's claims and harm

occurred in California. The privacy violations complained of herein resulted from Defendants' purposeful and tortious acts directed towards citizens of California while they were located within California. At all relevant times, Defendants targeted their goods and services to California citizens, and knew that their practices would directly result in collection of information from California citizens while those citizens browse www.titleist.com from devices located in California. Defendants chose to avail themselves of the business opportunities of marketing and selling their services in California and collecting real-time data from website visit sessions initiated by Californians while located in California, and the claims and harm alleged herein specifically arise from those activities.

3. Acushnet also knows that many users visit and interact with Acushnet's website while they are physically present in California. Both desktop and mobile versions of Acushnet's website allow a user to search for nearby retail partners 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). Users' employment of automatic location services in this way means that Acushnet 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 California statutory and common law.

4. 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. Further, California has the greatest material interest in protecting the citizens in the State of California and enforcing the California's laws given that the interception of Plaintiff's and Class Member's communications occurred from within the borders of the State.

INTRODUCTION

5. This is a class action brought against Acushnet for wiretapping the electronic communications of visitors to its website, www.titleist.com. Acushnet procures third-party vendors, such as FullStory, to embed snippets of JavaScript computer code ("Session Replay Code") on Acushnet'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 Acushnet's 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 Acushnet's request.

6. After intercepting and capturing the Website Communications, Acushnet and the Session Replay Providers use those Website Communications to

recreate website visitors' entire visit to www.titleist.com. The Session Replay Providers create a video replay of the user's behavior on the website and provide it to Acushnet for analysis. Acushnet'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 Acushnet's website for the entire duration of their website interaction.

7. Acushnet's conduct violates the Federal Wiretap Act, 18 U.S.C. §2510 *et. seq.* (the "Wiretap Act") and the California Invasion of Privacy Act ("CIPA"), Cal. Pen. Code §630, *et. seq.*, Cal. Pen. Code §§ 484, 496, and constitutes the torts of invasion of the privacy rights and intrusion upon seclusion of website visitors in relation to the unauthorized interception, collection, recording, and dissemination of Plaintiff's and Class Members' communications and data.

8. Plaintiff brings this action individually and on behalf of a class of all California citizens whose Website Communications were intercepted through Acushnet's procurement and use of Session Replay Code embedded on www.titleist.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

9. Plaintiff John Tanner is a citizen of the State of California, and at all times relevant to this action, resided and was a citizen of California. Plaintiff currently resides and is domiciled in Orange County, California. Plaintiff is a citizen of California.

10. Defendant Acushnet Company is corporation organized under the laws of Delaware, and its principal place of business in Fairhaven, Massachusetts. Defendant is a citizen of Massachusetts. Defendant Acushnet Company operates the brands Titleist—one of the most golf's leading performance equipment brands—and FootJoy—one of golf's leading performance wearable brands. Defendant Acushnet Company operates the brands' websites—www.titleist.com and www.footjoy.com.

11. Defendant Acushnet Holdings Corp. is a corporation organized under the laws of Delaware, and its principal place of business in Fairhaven, Massachusetts. Defendant is a citizen of Massachusetts. Upon information and belief, Acushnet Holdings Corp. is the parent company of Defendant Acushnet Company.

FACTUAL ALLEGATIONS

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

12. The "world's most valuable resource is no longer oil, but data."[1]

13. In 2022, 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 information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.[2] 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.[3]

14. 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

---

[1] *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.

[2] 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.

[3] *Id.*

behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[4]

15. 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."[5] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[6]

16. 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."[7]

---

[4] 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.

[5] 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.

[6] *Id.* at 25.

[7] *Id.*

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

17. 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."[8]

18. 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.[9] As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[10]

19. 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.

---

[8] 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/.

[9] *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.

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

20. 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.[11]

21. 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.[12]

22. 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.[13]

---

[11] *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/.

[12] *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/.

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

C. How Session Replay Code Works.

23. Session Replay Code, such as that implemented on www.titleist.com and www.footjoy.com, enables website operators to intercept, 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."[14]

24. 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 intercept and 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 submitting the data to the website operator.[15] As a result, website visitors "aren't just sharing data with the [web]site

[14] 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/.

[15] *Id.*

they're on . . . but also with an analytics service that may be watching over their shoulder."[16]

25. Session Replay Code works by inserting invisible 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 code waits and listens for specified events and communications, like a traditionally tapped phone, and each time an event triggers the code 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.

26. 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

[16] 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.

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.

27. 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.

28. 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 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."[17]

29. 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

[17] 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/.

captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.[18]

30. 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.

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

32. 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.

[18] *Id.*

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

34. 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.[19]

35. 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, are collected across all sites that the Session Replay Provider monitors.

36. 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.

---

[19] *Id.*; *see also FS.identify – Identifying users*, FullStory, https://help.fullstory.com/hc/en-us/articles/360020828113, (last visited Feb. 15, 2023).

37. 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.[20] 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."[21]

38. 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."[22]

---

[20] 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.

[21] 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/.

[22] 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.

39. 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.[23] This discovery was made just weeks after Air Canada said its app had a data breach, exposing 20,000 profiles.[24]

40. 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.[25] 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.[26]

---

[23] 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/.

[24] *Id.*

[25] Nitasha Tiku, The Dark Side of 'Replay Sessions' That Record Your Every Move Online, WIRED (Nov. 16, 2017), https://ecf.pawd.uscourts.gov/doc1/15719093861.

[26] Englehardt, *supra* note 18.

41. 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 was capturing credit card details, including the cardholder's name and billing address, the card's number, expiration, and security code from the Bonobos' website.[27]

42. 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.[28] 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."[29]

[27] Tiku, *supra* note 26.

[28] 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/.

[29] *Id.*

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

43. Acushnet operates the website www.titleist.com and www.footjoy.com, as well as all of their subpages. Acushnet designs, develops, manufactures, and distributes, golf products, operating two of golf's most well-known brands—Titleist and FootJoy.

44. Acushnet has committed itself to being one of the preferred and trusted partners of premium golf shops worldwide, such as on-course golf shops and specialty retailers throughout California.

45. The Titleist's website enables website visitors to browse for and purchase golf balls, golf clubs, and golf accessories. The Titleist website also enables website visitors to search for and schedule golf club fittings and search and find local golf club retail partners.

46. Likewise, the FootJoy website enables website visitors to browse and purchase various golf wearable accessories, including golf spikes and golf gloves. The FootJoy website also enables website visitors to search for and find local FootJoy dealers.

47. However, unbeknownst to the millions of individuals perusing Acushnet's websites, Acushnet intentionally procures and embeds various Session Replay Codes from Session Replay Providers on its website to track and analyze

website user interactions with www.titleist.com - and with www.footjoy.com, and their subpages.

48. One such Session Replay Provider that Acushnet procures is Hotjar.

49. Hotjar is the owner and operator of a Session Replay Code title Hotjar Tracking Code,[30] which records all website visitor actions, including information typed by the website users while on the website. Such information can include unique identifiers, names, email addresses, other similar personal information, race and gender, and records of products or services purchased.[31]

50. As a user interacts with any website with the Hotjar Tracking Code embedded, each mouse movement, scroll, click, and keyboard stroke is collected and sent to Hotjar.[32] While Hotjar suppresses keystrokes by default, replacing them with

---

[30] *How to Install Your Hotjar Tracking Code*, Hotjar, https://help.hotjar.com/hc/en-us/articles/115009336727-How-to-Install-Your-Hotjar-Tracking-Code (last visited Feb. 17, 2023).

[31] *Categories of Personal Information*, Hotjar, https://help.hotjar.com/hc/en-us/articles/1500000187901-Categories-of-Personal-Data (last visited Feb. 17, 2023).

[32] *Recordings: the complete guide*, Hotjar (last updated Jan. 31, 2023), https://www.hotjar.com/session-recordings/.

asterisks, websites can nevertheless override this function and collect keystrokes from text fields.[33]

51. Importantly, Hotjar offers a "User Lookup Tool" which allows a website to "search for personal data associated with individual users of [the] site, based on an email address or unique User ID."[34] Indeed, Hotjar enables websites to collect up to 100 user attributes, attributes that allow websites to deanonymize website visitors.[35] On such user attribute includes website visitors' IP addresses.[36]

---

[33] *How to Show Elements and keystrokes in Data Collections*, Hotjar, https://help.hotjar.com/hc/en-us/articles/115015563287-How-to-Show-Elements-and-Keystrokes-in-Data-Collection (last visited Feb. 17, 2023).

[34] Understanding the User Lookup Tool, Hotjar, https://help.hotjar.com/hc/en-us/articles/360001749014-Understanding-the-User-Lookup-Tool (last visited Feb. 17, 2023).

[35] *What Are user Attributes*, Hotjar, https://help.hotjar.com/hc/en-us/articles/4402892526487 (last visited Feb. 17, 2023).

[36] *Id.*

52. Once user attributes are being sent to Hotjar, websites can filter session replay recordings by user attributes and User ID and target users with specific surveys and feedback widgets.[37]

53. Hotjar also uses the information captured to create detailed heatmaps of a website that provide information about which elements of a website have high user engagement, how far website users scrolled on the website, and the total clicks within a given area on the website.[38]

54. As such, the Hotjar Tracking Code collects highly personal information and substantive communications that can be linked directly to a website user's identity as it monitors, records, and collects a website user's every move. And similar to other Session Replay Codes, the information collected and recorded by the Hotjar Tracking Code 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

---

[37] *Connecting Hotjar User IDs with Internal user IDs*, Hotjar, https://help.hotjar.com/hc/en-us/articles/360020755193-Connecting-Hotjar-User-IDs-with-Internal-User-IDs (last visited Feb. 17, 2023).

[38] *The Complete guide to Heatmaps*, Hotjar (last updated Feb. 13, 2023), https://www.hotjar.com/heatmaps/.

features, and other on-page elements.[39] Put differently, the information the Hotjar Tracking Code captures can be translated into a simulation video of how a user interacts with a website.

55. Given the breadth of information the Hotjar Tracking Code collects, including a website user's IP address and other personally identifying information, it is inevitable that Acushnet knows it is capturing, collecting, and recording the Website Communications of California residents.

56. Acushnet's procurement and use of Hotjar's Session Replay Code, and procurement and use of other Session Replay Codes through various Session Replay Providers, is a wiretap in violation of the Federal Wiretap Act, 18 U.S.C. §2510 *et. seq.* (the "Wiretap Act"), the California Invasion of Privacy Act ("CIPA"), Cal. Pen. Code §630, *et. seq.*, and Cal. Pen. Code §§ 484, 496, and constitutes the torts of invasion of the privacy rights and intrusion upon seclusion of website visitors in relation to the unauthorized interception, collection, recording, and dissemination of Plaintiff's and Class Members' communications and data. Indeed, once a website installs the Hotjar Tracking Code, that code acts as a secret wiretap that sends users'

[39] *See what your users see*, Hotjar, https://www.hotjar.com/product/recordings/ (last visited Feb. 17, 2023).

Website Communications to Hotjar in real time, instantly reporting every keystroke, movement, click, and/or moment of inactivity to the Hotjar server.

57. Acushnet knows it is capturing, collecting, and recording the Website Communications of California residents.

E. Plaintiff's and Class Members' Experience.

58. Plaintiff has visited www.titleist.com and certain of its subpages on his laptop computer and phone while in California prior to filing this action.

59. While visiting Acushnet's website, Plaintiff fell victim to Acushnet's unlawful monitoring, recording, and collection of Plaintiff's Website Communications with www.titleist.com prior to the filing of this action.

60. Unknown to Plaintiff, Acushnet procures and embeds Session Replay Code on its website. In particular, the Hotjar Tracking Code was operative on Acushnet's website and subpages during Plaintiff's visits to www.titleist.com.

61. During these visits by Plaintiff to www.titleist.com and its subpages, Plaintiff browed for products. Plaintiff communicated with Acushnet website by using his mouse to hover and click on certain products and typing search words into the search bar.

62. The Session Replay Code instantaneously captured his Website Communications throughout his visit. Indeed, through Acushnet's procurement of

Session Replay Code, Plaintiff's Website Communications were automatically and secretly intercepted by using Acushnet's website.

63. Further, without his consent, Acushnet procured Session Replay Providers to obtain certain information about his device and browser and create a unique ID and profile for him.

64. For example, when visiting www.titleist.com and its subpages, if a website user searches for products, that information is captured by the Session Replay Codes embedded on the website.

65. The wiretapping facilitated by the Session Replay Codes is ongoing during the visit and intercepts the contents of these communications between Plaintiff and Acushnet with instantaneous transmissions to the Session Replay Provider, in which only milliseconds were required to send a packet of event response data, which would indicate whatever the website user had just done.

66. Thus, on multiple occasions when Plaintiff visited Acushnet's website, the contents of his communications with the website were intercepted by Session Replay Code and simultaneously transmitted to Session Replay Providers.

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

68. Like Plaintiff, each Class member visited www.titleist.com (or www.footjoy.com and their subpages with Session Replay Code embedded in them,

and those Session Replay Codes intercepted the Class members' Website Communications with www.titleist.com or www.footjoy.com by sending hyper-frequent logs of those communications to Session Replay Providers.

69. Even if Acushnet 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's owner.

70. 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.

71. The Session Replay Code procured by Acushnet is an electronic, mechanical, or other analogous device for purposes of the Act in that the Session Replay Code, monitors, collects, and records the content of electronic computer-to-computer communications between Plaintiff's mobile computer and/or mobile device and the computer servers and hardware utilized by Acushnet to operate its website.

72. Alternatively, even if the Session Replay Code itself were not a device for purposes of the Act, the Session Replay Code is software designed to alter the

operation of a website visitor's computer or mobile phone by instructing the hardware components of that physical device to run the processes that ultimately intercept the visitor's communications and transmit them to the third-party Session Replay Provider, without the visitor's knowledge.

73. The Session Replay Code procured by Acushnet is not a website cookie, analytics tool, tag, web beacon, or other similar technology. Instead, the data collected by the Session Replay Code identified specific information inputted and content viewed, and thus revealed personalized and sensitive information about website visitors' Internet activity and habits. As such, by the very nature of its operation, the Session Replay Code is a device used to intercept electronic communications.

74. The Website Communications intentionally monitored, collected, and recorded by Acushnet was content generated through Plaintiff's and Class Members' use, interaction, and communication with Acushnet's website relating to the substance and/or meaning of Plaintiff's and Class Members' communications with the website, i.e., mouse clicks and movements, keystrokes, search terms, information inputted by Plaintiff and Class Members, and pages and content clicked on and viewed by Plaintiff and Class Members. This information is "content" and is not merely record information regarding the characteristics of the message that is generated in the course of the communication, nor is it simply information disclosed

in the referrer headers. The mere fact that Acushnet values this content, and monitors, intercepts and records it, confirms these communications are content that convey substance and meaning to Acushnet, and in turn, any Session Replay Provider that receives the intercepted information.

75. Acushnet's use of a session replay code to intercept Plaintiff's electronic communications in real-time did not facilitate, was not instrumental, and was not incidental to the transmission of Plaintiff's electronic communications with Acushnet's website.

76. Acushnet's use of session replay code was not instrumental or necessary to the operation or function of Acushnet's website or business.

77. Acushnet's use of a session replay code to contemporaneously intercept Plaintiff's electronic communications at the time of transmission was not instrumental or necessary to Acushnet's provision of any of its goods or services. Rather, the level and detail of information surreptitiously collected by Acushnet indicates that the only purpose was to gain an unlawful understanding of the habits and preferences of users to its website, and the information collected was solely for Acushnet's own benefit.

78. Plaintiff and the Class members had a reasonable expectation of privacy during their visits to Acushnet's website, which Acushnet violated by intentionally

monitoring and intercepting the content of their electronic communications with the website.

79. Acushnet's covert monitoring and interception of Plaintiff's and the Class members' electronic communications caused Plaintiff and the Class members harm, including violations of their substantive legal privacy rights, invasion of privacy, invasion of their rights to control information concerning their person, and/or the exposure of their private information. Moreover, Acushnet's practices caused harm and a material risk of harm to Plaintiff's and the Class Members' privacy and interest in controlling their personal information, habits, and preferences.

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

80. Plaintiff and Class Members did not provide prior consent to Acushnet's interception of their Website Communications, nor could they, as the interception begins *immediately* upon arriving at www.titleist.com or www.footjoy.com and/or their subpages.

81. Acushnet 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 Acushnet is using Session Replay Code to monitor, collect, and record their Website

Communications because the Session Replay Code is seamlessly incorporated and embedded into Acushnet's website.

82. While Acushnet purports to maintain privacy policies on www.titleist.com and www.footjoy.com, the privacy policies are insufficient for Plaintiff to furnish prior consent. First, because the wiretapping begins the moment a website user arrives on www.titleist.com, www.footjoy.com, or one of their subpages, Plaintiff and Class Members had no opportunity to review the privacy policies before they were wiretapped and therefore could not have opted out of or prevented the wiretapping before it occurred. Additionally, a reasonable person would not be on notice of the terms of privacy policies by way of normal interaction with the websites. Acushnet's privacy policies are on www.titleist.com and www.footjoy.com are buried at the very bottom of the websites in small font that is unobtrusive and easy to overlook. As such a reasonable person could browse for products on Acushnet's websites without ever being on notice of the purported privacy policies.

83. Similarly, Plaintiff and Class Members did not assent to the purported "forum selection" or "choice of law" clauses contained in Acushnet's terms of use. At no point during a www.titleist.com, www.footjoy.com, and/or their subpages is a website visitor asked to agree or even view Acushnet's terms of use. Further, Acushnet's terms of use are buried at the very bottom of the website in small font

that is unobtrusive and easy to overlook. As such, a reasonable person could browse for products on Acushnet's websites without ever being on notice of the purported terms of use. Moreover, because the only mechanism Acushnet offers for declining agreement to these terms is avoiding use of the websites altogether, no person who has ever visited the websites or any of their subpages is ever given an actual opportunity to decline or avoid these terms. In order to even navigate to the place where the terms are displayed, a visitor must use the site in a way that Acushnet deems to be acceptance of the terms.

CLASS ACTION ALLEGATIONS

84. 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 in California through the use of Session Replay Code embedded in www.titleist.com and in www.footjoy.com.

85. 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.

86. **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 Acushnet or the Session Replay Providers.

87. **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 Acushnet's website visitors' Website Communications; (b) whether Acushnet intentionally discloses the intercepted Website Communications of its website users; (c) whether Defendant acquires the contents of website users' private Website Communications without their consent; (d) whether Plaintiff and Class Members had a reasonable expectation of privacy in their Website communications; (e) whether Defendant's conduct violates the Federal Wiretap Act, 18 U.S.C. §2510, *et. seq.,* (the "Wiretap Act"), the California Invasion of Privacy Act ("CIPA"), the Cal. Pen. Code §630, *et. seq.,* Cal. Penal Code §§ 484 and 496, and/or constitutes a tortious invasion of privacy and/or intrusion on seclusion; (f) whether Plaintiff and the Class members are entitled to equitable relief; and (g) whether Plaintiff and the Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

88. **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.

89. **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 his 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.

90. **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.

91. **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.

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

COUNT I

Violation of Federal Wiretap Act

18 U.S.C. §2510 *et. seq.*

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

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

95. The Federal Legislature passed the Wiretap Act to protect the privacy of the people of the United States. The Wiretap Act is very clear in its prohibition against intentional unauthorized taping or interception of any wire, oral, or electronic communication. In addition to other relevant sections, the Wire Tap Act states that any person who; "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" has violated the act. 18 U.S.C. §2511.

96. Acushnet intercepted Plaintiff's and Class Members' electronic communications and tracking their communications and interactions with Acushnet's website.

97. "Intercept" is defined as any "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 U.S.C. §2510.

98. "Contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510.

99. "Person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510.

100. "Electronic Communication" is defined as "[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system." 18 U.S.C. § 2510.

101. Acushnet is a person for purposes of the Act because it is a corporation.

102. Session Replay Code like that procured by Acushnet is a "device" used for the "acquisition of the contents of any wire, electronic, or oral communication" within the meaning of the Act. Courts have held that software constitutes a "device" for purposes of applying wiretap statutes. *See, e.g.*, *United States v. Barrington*, 648 F.3d 1178, 1203 (11th Cir. 2011) (accepting that a keylogger software could be considered a device); *Luis v. Zang*, 833 F.3d 619, 630 (6th Cir. 2016) (accepting that a software could be a "device" for the purpose of the Wiretap Act); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1087 (N.D. Cal. 2015) (concluding that a software was an "electronic, mechanical or other device"); *Klumb v. Goan*, 884 F. Supp. 2d 644, 661-62 (E.D. Ten. 2012) (analyzing spyware software as a device under Wiretap Act); *Shefts v. Petrakis*, 2012 WL 4049484, at *8-9 (C.D. Ill. 2012) (analyzing software as a device under the Wiretap Act).

103. Alternatively, even if the Session Replay Code itself were not considered a "device" under the Act, Acushnet ultimately "uses" the physical computers and mobile phones of Plaintiff and Class members by sending the Session

Replay Code to those devices. In turn, the Session Replay Code instructs those devices to run the physical processes necessary to accomplish the interception of Plaintiff's and Class members' communications and transmission of those communications to the third-party Session Replay Providers.

104. Acushnet intentionally procures and embeds Session Replay Code on its website to spy on—automatically and secretly—and to intercept its website visitors' electronic interactions communications with Acushnet in real time.

105. Plaintiff's and Class members' intercepted Website Communications constitute the "contents" of electronic communication[s]" within the meaning of the Act.

106. Plaintiff's and Class members' electronic communications are intercepted contemporaneously with their transmission.

107. Plaintiff's interactions with Acushnet's website and its subpages, including his directional, selection, and clicking actions (using a mouse, arrow keys, or a finger), the display of information coming from Acushnet and directed to Plaintiff, and Plaintiff's entry of text into search form fields, were all exchanges of electronic communications between Plaintiff and Acushnet.

108. Plaintiff's and Class members' intercepted Website Communications therefore constitute the "contents" of electronic communication[s]" within the meaning of the Act.

109. By operation of the Session Replay Code on Plaintiff's device, these forms of communications were captured continuously, within milliseconds, and immediately transmitted to and acquired by third-party Session Replay Providers.

110. Plaintiff and Class members did not consent to having their Website Communications wiretapped.

111. Acushnet uses or attempts to use the electronic communications it views and intercepts in order to market its services and goods to Plaintiff and the Class members.

112. Plaintiff and the Class members had a reasonable expectation of privacy during their visits to Defendant's website, which Defendant violated by intentionally monitoring and intercepting their electronic communications with the website.

113. Plaintiff brings this action for every violation of the Wiretap Act which provides for statutory damages of the greater $10,000 or $100 per day for each violation of 18 U.S.C. §2510 et seq under 18 U.S.C. §2520.

114. Acushnet'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.

COUNT II

Unlawful Wiretapping and Interception of Electronic Communication

Cal. Pen. Code § 630

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

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

117. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Pen. Code § 630, *et seq.*, and defines its purpose as:

> 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.

See Cal. Pen. Code § 630.

118. Acushnet intercepted components of Plaintiff's and Class Members' private electronic communications and transmissions when Plaintiff and other class members accessed Acushnet's website from within the State of California.

119. To establish liability under section 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner" does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument of any internal telephonic communication system,
>
> **Or**
>
> 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 the state,
>
> **Or**
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> **Or**
>
> 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.

120. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *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); *Bradley v. Google, Inc*., 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, --- F.3d --- 2020 WL 1807978 (9th Cir. Apr. 9, 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history).

121. Acushnet's use of the "session replay" spyware is a "machine, instrument, contrivance, or . . . other manner" used to engage in the prohibited conduct at issue here.

122. At all relevant times, Acushnet'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.

123. By using the "session replay" spyware to track, record, and attempt to learn the contents of Plaintiff's and Class Members' electronic communications, Acushnet intentionally tapped, electrically or otherwise, the lines of internet communication of Plaintiff and Class Members.

124. Plaintiff, and each Class Member, visited and/or interacted with Acushnet's website while in California.

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

126. Plaintiff and Class members did not consent to, authorize, or know about Acushnet's intrusion at the time it occurred. Plaintiff and Class members never agreed that Acushnet could intercept, read, learn, collect or disclose the content of their Website Communications.

127. 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.

128. Acushnet intentionally intrudes on Plaintiff's and Class members' private life, seclusion, or solitude, without consent, in that Acushnet 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 Acushnet without engaging in this practice. Acushnet directly participated in the interception, reading, and/or learning of the contents of the communications between Plaintiff, Class members and California-based web entities.

129. The information Acushnet 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.

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

131. Plaintiff and Class members were harmed and suffered loss by Acushnet's wrongful conduct and violations, including but not limited to, violation of the right to privacy and confidentiality of their electronic communications.

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

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

134. As a result of the above violations and pursuant to CIPA section 637.2, Acushnet 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."

135. Acushnet's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Acushnet'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.

136. 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 Acushnet.

COUNT III

Statutory Larceny

Cal. Pen. Code § 484 and 496

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

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

139. Section 496(a) of the California Penal Code prohibits the obtaining of property "in any manner constituting theft." Cal. Pen. Code § 496(a).

140. Cal. Pen. Code § 484 defines theft as:

> Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

Cal. Pen. Code § 484.

141. Accordingly, the Cal. Pen. Code, specifically, Section 484, definition of "theft" includes obtaining property by false pretenses.

142. Acushnet intentionally utilized software in a manner that obtained the information of Plaintiff unbeknownst to Plaintiff, and without his consent, and in doing so, deceived Plaintiff into providing information to Acushnet.

143. Thus, Acushnet acted in a manner that constitutes theft and/or false pretenses.

144. Acushnet stole, took and/or fraudulently appropriated Plaintiff's information without his consent.

145. Acushnet concealed, aided in the concealing, and/or utilized Plaintiff's information for commercial purposes and to Acushnet's direct financial benefit, as the reasonable and fair market value of the unlawfully obtained data can be determined in the marketplace.

146. As a result, Plaintiff and the Class have suffered damages in an amount to be determined at trial.

COUNT IV

Invasion of Privacy – Intrusion upon Seclusion

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

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

149. California recognizes a common law right to privacy and the tort of invasion of privacy/intrusion on seclusion and Acushnet has invaded Plaintiff's right to privacy contained on various personal computing devices, including, but limited to, web-browsing history.

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

151. Acushnet's actions constitute a serious invasion of privacy in that its actions invade a federally protected zone of privacy and seclusion, violate several federal and state laws; and invaded the privacy of thousands of individuals without their consent, all while profiting from these actions, which demonstrates Acushnet's legitimate business interest in obtaining this information.

152. This tracking was non-consensual and was an intentional interception of Plaintiff and the Class's communications.

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

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

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

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

157. Given the monetary value of individual personal information, Acushnet deprived Plaintiff and Class members of the economic value of their interactions with Acushnet's website, without providing proper consideration for Plaintiff's and Class members' property.

158. Acushnet has improperly profited from its invasion of Plaintiff's and Class members' privacy in its use of their data for its economic value.

159. As a result, Plaintiff and Class Members have suffered damages, including, but not limited to violation of their right to privacy and loss of value of their personal information.

160. Acushnet's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Acushnet'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 Acushnet's past conduct was unlawful, as alleged herein;

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

E. Enjoining Acushnet 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 as may be appropriate;

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

Dated: February 27, 2023

Respectfully submitted,

/s/ John J. Nelson

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Tel.: (858) 209-6941
jnelson@milberg.com

MaryBeth V. Gibson *(pro hac vice forthcoming)*
THE FINLEY FIRM, P.C.
3535 Piedmont Road
Building 14, Suite 230
Atlanta, Georgia 30305
T: (404) 978-6971
F: (404) 320-9978
MGibson@TheFinleyFirm.com