Joshua B. Swigart (SBN 225557)
Josh@SwigartLawGroup.com
SWIGART LAW GROUP, APC
2221 Camino del Rio S, Ste 308
San Diego, CA 92108
P: 866-219-3343

Daniel G. Shay (SBN 250548)
DanielShay@TCPAFDCPA.com
LAW OFFICE OF DANIEL G. SHAY
2221 Camino del Rio S, Ste 308
San Diego, CA 92108
P: 619-222-7429

Attorneys for Plaintiff and The Putative Class

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

DAVID KAUFFMAN, individually and on behalf of others similarly situated, Plaintiff, vs. THE HOME DEPOT, INC., Defendant.	CASE NO: '23CV0259 JLS AHG CLASS ACTION COMPLAINT FOR DAMAGES FOR VIOLATIONS OF: 1. THE WIRETAP ACT, 18 U.S.C. § 2510 ET SEQ 2. THE CALIFORNIA INVASION OF PRIVACY ACT, CAL. PEN. CODE § 631 3. THE CALIFORNIA INVASION OF PRIVACY ACT, CAL. PEN. CODE § 632 4. THE CALIFORNIA INVASION OF PRIVACY ACT, CAL. PEN. CODE § 632.7 JURY TRIAL DEMANDED

INTRODUCTION

1. David Kauffman. ("Plaintiff"), individually and on behalf of all other similarly situated consumers ("Class Members"), brings this action for damages and injunctive relief against The Home Depot, Inc. ("Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, related entities for violations of 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 §§ 631, 632 and 632.7, in relation to the unauthorized interception, collection, recording, and dissemination of Plaintiff's and Class Members' communications and data.

2. 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 tapping 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

3. The California State Legislature passed CIPA to protect the right of privacy of the people of California. The California Penal Code is very clear in its prohibition against unauthorized tap or connection without the consent of the other person:

> "Any person who, by means of any machine, instrument, or contrivance, or any other matter, intentionally taps, or makes any unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable. Or instrument of any internal telephonic communication system, or who willfully and without 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 [violates this section]." Cal. Penal Code § 631(a)
>
> "A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars ($2,500) per violation, or imprisonment in a county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment. If the person has previously been convicted of a violation of this section or Section 631, 632.5, 632.6, 632.7, or 636, the person shall be punished by a fine not exceeding ten thousand dollars ($10,000) per violation, by imprisonment in a county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment."
> Cal. Penal Code § 632(a)
>
> "Every person who, without the consent of all parties to a communication, intercepts or receives and intentionally records, or assists in the interception or reception and intentional recordation of, a communication transmitted between two cellular radio telephones, a cellular radio telephone and a landline telephone, two cordless telephones, a cordless telephone and a landline telephone, or a cordless telephone and a cellular radio telephone, shall be punished by a fine not exceeding two thousand five hundred dollars ($2,500), or by imprisonment in a county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment. If the person has been convicted previously of a violation of this section or of Section 631 , 632, 632.5, 632.6, or 636, the person shall be punished by a fine not exceeding ten thousand dollars ($10,000), by imprisonment in a county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment."
> Cal. Penal Code § 632.7(a)

4. This case stems from Defendant's unauthorized interception and connection to Plaintiff's and Class Members' electronic communications through the use of

"session replay" spyware that allowed Defendant to record, read, learn the contents of, and make reports on Plaintiff's and Class Members' interactions on Defendant's website including search terms they entered.

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

6. Plaintiff also brings this action for every violation of California Penal Code §§ 631, 632 and 632.7 which provides for statutory damages of $5,000 for each violation, pursuant to Cal. Pen. Code § 637.2(a)(1).

7. As discussed in detail below, Defendant utilized session replay spyware to intercept Plaintiff's and the Class Members' electronic computer-to-computer electronic communications. Defendant procures third-party vendors, such as Quantum Metric, to embed JavaScript computer code on Defendant's website, which then deploys on each website visitor's internet browser for the purpose of watching, intercepting, and recording the website visitor's electronic communications with Defendant's website.

8. Defendant deployed the session replay spyware at the moment Plaintiff and Class Members visited Defendant's website, and its use allowed Defendant to intercept, read, record, and learn the contents of Plaintiff's and Class Members' interactions with Defendant's website, including how Plaintiff and Class Members interacted with the website, mouse movements and clicks, keystrokes, search terms, information inputted into the website, and pages and content viewed while visiting the website. Defendant intentionally tapped and made unauthorized interceptions and connections to Plaintiff's and Class Members' electronic communications to read and understand movement on the website, as well as everything Plaintiff and Class Members did on those pages, *e.g.*, both the information inputted and what Plaintiff and Class Members searched for, looked at, and clicked on.

9. After intercepting and capturing Plaintiff's and Class Members' communications, Defendant and its third-party vendor(s) use those communications to view in real-time users' entire visit to Defendant's website. The surreptitious interception, recording, and review of Plaintiff's and Class Members' communications is the electronic equivalent of "looking over the shoulder" of each visitor to the website for the entire duration of the user's website interaction.

10. Defendant made these unauthorized interceptions, connections and recordings without the knowledge or prior consent of Plaintiff or Class Members.

11. "Technological advances[,]" such as Defendant's use of session replay technology, "provide 'access to a category of information otherwise unknowable' and 'implicate privacy concerns' in a manner different from traditional intrusions as a 'ride on horseback' is different from a 'flight to the moon.'" *Patel v. Facebook, Inc.,* 932 F.3d 1264, 1273 (9th Cir. 2019) (quoting *Riley v. California*, 573 U.S. 373, 393 (2014)).

12. Jonathan Cherki, the CEO of a major "session replay" spyware company – while discussing the merger of his company with another session replay provider – publicly exposed why companies like Defendant engage in learning the contents of visits to their websites: "The combination of Clicktale and Contentsquare heralds an unprecedented goldmine of digital data that enables companies to interpret and predict the impact of any digital element – including user experience, content, price, reviews and product – on visitor behavior[.]"[1] Mr. Cherki added that, "this unique data can be used to activate custom digital experiences in the moment via an ecosystem of over 50 martech partners. With a global community of customer and partners, we are accelerating the

[1] https://www.prnewswire.com/news-releases/contentsquare-acquires-clicktale-to-create-the-definitive-global-leader-in-experience-analytics-300878232.html

interpretation of human behavior online and shaping a future of addictive customer experience."[2]

13. Unlike typical website analytics services that provide aggregate statistics, the session replay technology utilized by Defendant is intended to record and playback individual browsing session, as if someone is looking over Plaintiff's or a Class Members' shoulder with a camera set to record when visiting Defendant's website. The technology also permits companies like Defendant to view the interactions of visitors on Defendant's website in live, real-time.

14. The extent and detail collected by users of the technology, like Defendant, far exceeds Plaintiff's and Class Members' expectations when visiting websites like Defendant's. The technology not only allows the tapping and unauthorized connection of a visitor's electronic communication with the website, but also allows Defendant to create a detailed profile for each visitor to the site.

15. Moreover, the collection of page content allows sensitive personal information displayed on a page to be shared with others. This exposes website visitors to potential identity theft, online scams, and other unwanted behavior.

16. In 2019, Apple warned application developers using "session replay" technology that they were required to disclose such action to their users, or face being immediately removed from the Apple Store: "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."[3]

17. Consistent with Apple's concerns, countless articles have been written about the privacy implications of recording user interactions during a visit to a website, including:

---

[2] *Id*

[3] https://techcrunch.com/2019/02/07/apple-glassbox-apps/

(a) ***The Dark Side of 'Replay Sessions' That Record Your Every Move Online***, located at https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/;

(b) ***Session-Replay Scripts Disrupt Online Privacy in a Big Way***, located at https://www.techrepublic.com/article/session-replay-scripts-are-disrupting-online-privacy-in-a-big-way/;

(c) ***Are Session Recording Tools a Risk to Internet Privacy?*** located at https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/

(d) ***Session Replay is a Major Threat to Privacy on the Web***, located at https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720;

(e) ***Popular Websites Record Every Keystroke You Make and Put Personal Information and Risk***, located at https://medium.com/stronger-content/popular-websites-record-every-keystroke-you-make-and-put-personal-information-at-risk-c5e95dfda514; and

(f) ***Website Owners can Monitor Your Every Scroll and Click***, located at https://www.digitalinformationworld.com/2020/02/top-brands-and-websites-can-monitor-your-every-scroll-and-click.html

18. In sum, Defendant illegally tapped, made an unauthorized connection to, intercepted and recorded Plaintiff's and Class Members' electronic communications when they visited Defendant's website. Defendant infringed upon Plaintiff's and Class Members' rights to privacy codified in the Wiretap Act and CIPA.

19. Plaintiff makes these allegations on information and belief, with the exception of those allegations that pertain to Plaintiff, or to Plaintiff's counsel, which Plaintiff alleges on personal knowledge.

20. Unless otherwise stated, all the conduct engaged in by Defendant took place in California.

21. All violations by Defendant were knowing, willful, and intentional, and Defendant did not maintain procedures reasonably adapted to avoid such violations.

22. The use of Defendant's name in this Complaint includes all agents, employees, officers, members, directors, heirs, successors, assigns, principals, trustees, sureties, subrogees, representatives, and insurers of the named Defendant.

PARTIES

23. Plaintiff is, and at all times mentioned herein was, a natural person and resident of the State of California and the County of San Diego.

24. Defendant is, and at all times mentioned herein was, a Delaware corporation with its principal place of business located in Georgia.

25. At all times relevant herein Defendant conducted business in the State of California, in the County of San Diego, within this judicial district.

JURISDICTION & VENUE

26. This Court has original subject matter jurisdiction under 28 U.S.C. § 1331 because this action arises out of Defendant's violations of the Wiretap Act, 18 U.S.C. §2510 et seq.

27. Jurisdiction is also proper under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because Plaintiff, a resident of the State of California, seeks relief on behalf of (1) a national class and (2) three California classes, which will result in at least one Class Member belonging to a different state than Defendant, a Delaware Corporation with its principal place of business in Georgia.

28. Plaintiff is requesting statutory damages of the greater of $10,000 or $100 per day for each violation of 18 U.S.C. § 2510 et seq and $5,000 per violation of Cal. Pen. Code §631, 632 and 632.7, which when aggregated among a proposed class number in the hundreds of thousands, exceeds the $5,000,000 threshold for federal court jurisdiction under CAFA.

///

29. Therefore, both diversity jurisdiction and the damages threshold under CAFA are present, and this Court has subject matter jurisdiction.

30. 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. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of California, such as Plaintiff, while they were located within California. At all relevant times, Defendant did business over the internet with residents of California, including Plaintiff, and entered into contracts with residents of California for the sale of goods. Defendant knew that its eavesdropping practices would directly result in the real-time viewing and collection of information from California citizens while those citizens were engaging in commercial activity on Defendant's website. Defendant chose to benefit from marketing and selling its goods in California. It then viewed real-time data from the website visits initiated by Californians while located in California. The claims alleged herein arise from those activities.

31. Defendant also knows that many users visit and interact with Defendant's websites while they are physically present in California. Many Californians purchase goods on Defendant's site and Defendant ships the goods to their California addresses. Another way Defendant knows a consumer is located in California is through location-determining tools that track and analyze users' IP addresses, without requiring the user to manually input a physical address. The employment of automatic location services in this way means that Defendant is continuously aware that its website is being visited by people located in California to buy Defendant's products in California, and that such website visitors are being wiretapped and recorded in violation of California statutory and common law, causing harm to California citizens.

32. In addition, Defendant included California-specific provisions in its privacy policies in recognition that California citizens would be using Defendant's

website while in California and that such use, as well as Defendant's own conduct, was subject to California law[4].

33. Venue is proper pursuant to 28 U.S.C. § 1391 for the following reasons: (i) the conduct complained of herein occurred within this judicial district; and (ii) Defendant conducted business within this judicial district at all times relevant.

FACTUAL ALLEGATIONS

34. Defendant owns and operates the following website: www.homedepot.com.

35. Over the past year and beyond, Plaintiff and Class Members visited Defendant's website.

36. Plaintiff was in California during each visit to Defendant's website.

37. As soon as Defendant's website loaded on Plaintiff's computer and cell phone, Defendant's "session replay" software caused Plaintiff's devices to begin transmitting electronic communications in the form of instructions to Defendant's computer servers utilized to operate its website. The commands were sent as messages indicating to Defendant what search terms were entered and what content was being viewed, clicked, requested, and inputted by Plaintiff.

38. The communications sent by Plaintiff to Defendant's servers included, but were not limited to, the following actions while on Defendant's website: search terms, mouse clicks and movements, keystrokes, information input by Plaintiff, pages and content viewed by Plaintiff, scroll movements, and copy and paste actions. Defendant tracked and recorded similar communications and actions by other Class Members.

39. Defendant responded to Plaintiff's and Class Members' electronic communications by supplying – through its website – the information requested by Plaintiff and Class Members. *Revitch v. New Moosejaw, LLC,* U.S. Dist.

[4] https://www.homedepot.com/privacy/California-Privacy-Rights-and-Report

LEXIS 186955, at *3 (N.D. Cal. 2019) ("This series of requests and responses – whether online or over the phone – is communication.").

40. Defendant used session replay software which enabled it to see the screens of Plaintiff and Class Members while they were on Defendant's website.

41. The "sessions" were intercepted, recorded, and shared by, or with, Quantum Metric or another third-party vendor conspiring with Defendant.

42. Defendant continuously operates at least one "session replay" JavaScript in its HTML code in partnership with the script's provider, Quantum Metric, or another provider ("Session Replay Provider" or "Provider").

43. Defendant installed the Provider's session replay spyware onto its server(s) and inserted the JavaScript into the HTML code of its website.

44. When consumers visit Defendant's website, the JavaScript immediately loads onto their device, from Defendant's site, and is stored in their device's cache or temporary internet files.

45. Like a parasite or a virus, the spyware then monitors and records every communication the device sends to, and receives from, Defendant's servers while the consumer browses the site.

46. Once tapped, the communications are still allowed to travel their normal path between the consumer's device and Defendant's servers, but the communications are copied and sent to the Provider's servers as well. Like traditional wiretapping, the communication still goes through, despite the tapping and recording. The consumer is completely unaware of what is happening.

47. The recordings are stored on the Provider's servers where Defendant, or other third parties, can access them real time or later.

48. The spyware is not purchased from the Provider then used solely by its user without any involvement from the Provider.

49. The Provider plays an active role in the use of its spyware by (1) inserting its JavaScript into the HTML code on Defendant's website (2) causing the

JavaScript to download onto consumers' devices when they visit the site (3) using the script to tap the consumers' communications to and from the site (4) sending copies of the communications to its servers (5) allowing Defendant, and potentially others, to access the sessions real time or later.

50. This was all done at the direction of Defendant who procured the Provider to tap, intercept and record the communications. The acts were done with the aid and agreement of Defendant in conspiracy with the Provider.

51. Plaintiff and Class Members reasonably expected that visits to Defendant's website would be private, and that Defendant, or its co-conspirator, would not be intercepting, tapping, connecting to, recording, or otherwise attempting to understand their communications with Defendant's website, particularly because Defendant failed to present Plaintiff and Class Members with a pop-up disclosure or consent form alerting Plaintiff that the visits to the website were monitored and recorded by Defendant.

52. Plaintiff and Class Members reasonably believed their interactions with Defendant's website were private and would not be recorded or monitored for a later playback by Defendant or monitored live while Plaintiff and Class Members were on its website.

53. The Session Replay Provider is not a provider of wire or electronic communication services, or an internet service provider.

54. Defendant's use of session play spyware was not instrumental or necessary to the operation or function of Defendant's website or business.

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

56. Defendant's use of a session replay spyware to intercept Plaintiff's and Class Members' electronic communications did not facilitate, was not instrumental, and was not incidental to the transmission of Plaintiff's and Class Members' electronic communications with Defendant's website.

57. During one or more of Plaintiff's and Class Members' visits to Defendant's website, Defendant utilized its session replay spyware to intercept the substance of Plaintiff's and Class Members' electronic communications with its website, intentionally and contemporaneously, including mouse clicks and movements, keystrokes, search terms, information input by Plaintiff, pages and content viewed, scroll movements, and copy and paste actions. In other words, Defendant tapped and made unauthorized connections to the electronic communications of Plaintiff and Class Members made during visits to Defendant's website.

58. The relevant facts regarding the full parameters of the communications Defendant intercepted and the extent of how the connections occurred are solely within the possession and control of Defendant.

59. The session replay spyware utilized by Defendant is not a website cookie, standard analytics tool, web beacon, or other similar technology.

60. Unlike harmless collection of an internet protocol address, the data collected by Defendant identified specific information inputted and content viewed, and thus revealed personalized and sensitive information about Plaintiff's and Class Members' internet activity and habits.

61. The electronic communications Defendant intentionally intercepted was content generated through Plaintiff's use, interaction, and communication with Defendant's website relating to the substance, purport, and meaning of Plaintiff's and Class Members' communications with the website.

62. The electronic communications Defendant intercepted were not generated automatically and were not incidental to other consumer communications.

///

63. The session replay spyware utilized by Defendant allowed Defendant to learn the contents of communications of Plaintiff and Class Members in a manner that was undetectable to them.

64. Defendant's session replay spyware recorded and shared Plaintiff's and Class Members' communications and played them back and analyzed them for business purposes.

65. Defendant never sought consent, and Plaintiff and Class Members never provided consent, for Defendant's unauthorized access to their electronic communications.

66. Plaintiff and Class Members did not have a reasonable opportunity to discover Defendant's unlawful and unauthorized connections because Defendant did not disclose its actions nor seek consent from Plaintiff or Class Members prior to making the unauthorized connections to the electronic communications through the session replay spyware.

STANDING

67. Defendant's conduct constituted invasions of privacy because it disregarded Plaintiff's statutorily protected rights to privacy, in violation of the Wiretap Act and CIPA.

68. Defendant caused Plaintiff to (1) suffer invasions of legally protected interests. (2) The invasions were concrete because the injuries actually existed for Plaintiff and continue to exist every time Plaintiff visits Defendant's website. The privacy invasions suffered by Plaintiff and Class Members were real and not abstract. Plaintiff and Class Members have a statutory right to be free from interceptions of their communications. The interceptions Defendant performed were meant to secretly spy on Plaintiff to learn more about Plaintiff's behavior. Plaintiff and Class Members were completely unaware they were being observed. Plaintiffs' injuries were not divorced from concrete harm in that privacy has long been protected in the form of trespassing laws and the Fourth Amendment of the U.S. Constitution for example. Like here, an unreasonable search may not cause

actual physical injury, but is considered serious harm, nonetheless. (3) The injuries here were particularized because they affected Plaintiff in personal and individual ways. The injuries were individualized rather than collective since Plaintiff's unique communications were examined without consent during different website visits on separate occasions. (4) Defendant's past invasions were actual and future invasions are imminent and will occur next time Plaintiff visits Defendant's website. Defendant continues to intercept communications without consent. A favorable decision by this court would redress the injuries of Plaintiff and each Class.

TOLLING

69. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know, and had no way of knowing, that Plaintiff's information was intercepted, because Defendant kept this information secret.

CLASS ACTION ALLEGATIONS

70. Plaintiff brings this lawsuit as a class action on behalf of Plaintiff and Class Members of four proposed Classes under F.R.C.P. 23.

71. Plaintiff proposes the following Classes, consisting of and defined as follows:

> Class One (18 U.S.C. § 2511)
> All persons in the United States whose communications were intercepted by a person Defendant procured.
>
> Class Two (Cal. Penal Code § 631)
> All persons in California whose communications were tapped by a person Defendant aided, agreed with, employed, or conspired to tap.
>
> Class Three (Cal. Penal Code § 632)
> All persons in California whose confidential communications were recorded by Defendant or its agents.
>
> Class Four (Cal. Penal Code § 632.7)
> All persons in California whose cellular communications were recorded by Defendant or its agents.

72. Excluded from each Class are: (1) Defendant, any entity or division in which Defendant has a controlling interest, and its legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) those persons who have suffered personal injuries as a result of the facts alleged herein. Plaintiff reserves the right to redefine each Class and to add subclasses as appropriate based on discovery and specific theories of liability.

73. **Numerosity**: The Class Members are so numerous that joinder of all members would be unfeasible and impractical. The membership of each Class is currently unknown to Plaintiff at this time; however, given that, on information and belief, Defendant accessed millions of unique computers and mobile devices, it is reasonable to presume that the members of each Class are so numerous that joinder of all members is impracticable. The disposition of their claims in a class action will provide substantial benefits to the parties and the Court.

74. **Commonality**: There are common questions of law and fact as to Class Members that predominate over questions affecting only individual members, including, but not limited to:

- Whether Defendant intercepted any communications with Class Members;
- Whether Defendant had, and continues to have, a policy during the relevant period of intercepting digital communications of Class Members;
- Whether Defendant's policy or practice of intercepting Class Members digital communications constitutes a violation of 18 U.S.C. § 2520;
- Whether Defendant's policy or practice of intercepting Class Members digital communications constitutes a violation of Cal.

Penal Code § 631;

- Whether Defendant's policy or practice of recording Class Members confidential digital communications constitutes a violation of Cal. Pen. Code § 632;
- Whether Defendant's policy or practice of recording Class Members digital communications constitutes a violation of Cal. Pen. Code § 632.7;
- Whether Plaintiff and Class Members were aware of Defendant's session replay spyware and had consented to its use.

75. **Typicality**: Plaintiff's and Class Members' electronic communications were intercepted, unlawfully tapped and recorded without consent or a warning of such interception and recording, and thus, the injuries are also typical to Class Members.

76. Plaintiff and Class Members were harmed by the acts of Defendant in at least the following ways: Defendant, either directly or through its agents, illegally intercepted, tapped, recorded, and stored Plaintiff and Class Members' electronic communications, and other sensitive personal data from their digital devices with others, and Defendant invading the privacy of Plaintiff and Class Members. Plaintiff and Class Members were damaged thereby.

77. **Adequacy**: Plaintiff is qualified to, and will, fairly and adequately protect the interests of each Class Member with whom Plaintiff is similarly situated, as demonstrated herein. Plaintiff acknowledges that Plaintiff has an obligation to make known to the Court any relationships, conflicts, or differences with any Class Member. Plaintiff's attorneys, the proposed class counsel, are well versed in the rules governing class action discovery, certification, and settlement. In addition, Plaintiff's attorneys, the proposed class counsel, are versed in the rules governing class action discovery, certification, and settlement. The proposed class counsel is experienced in handling claims involving consumer actions and

violations of the Wiretap Act and California Penal Code § 631. Plaintiff has incurred, and throughout the duration of this action, will continue to incur costs and attorneys' fees that have been, are, and will be, necessarily expended for the prosecution of this action for the substantial benefit of each Class Member. Plaintiff and proposed class counsel are ready and prepared for that burden.

78. **Predominance**: Questions of law or fact common to the Class Members predominate over any questions affecting only individual members of each Class. The elements of the legal claims brought by Plaintiff and Class Members are capable of proof at trial through evidence that is common to each Class rather than individual to its members.

79. **Superiority**: A class action is a superior method for the fair and efficient adjudication of this controversy because:

a. Class-wide damages are essential to induce Defendant to comply with Federal and California law.

b. Because of the relatively small size of the individual Class Members' claims, it is likely that only a few Class Members could afford to seek legal redress for Defendant's misconduct.

c. Management of these claims is likely to present significantly fewer difficulties than those presented in many class claims.

d. Absent a class action, most Class Members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law.

e. Class action treatment is manageable because it will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would endanger.

f. Absent a class action, Class Members will continue to incur

damages, and Defendant's misconduct will continue without remedy.

80. Plaintiff and the Class Members have suffered, and will continue to suffer, harm and damages as a result of Defendant's unlawful and wrongful conduct. A class action is superior to other available methods because as individual Class Members have no way of discovering that Defendant intercepted and recorded the Class Member's electronic communications without Class Members' knowledge or consent.

81. Each Class may also be certified because:

- The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudication with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant;
- The prosecution of separate actions by individual Class Members would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and
- Defendant has acted, or refused to act, on grounds generally applicable to each Class, thereby making appropriate final and injunctive relief with respect to the members of each Class as a whole.

82. This suit seeks only damages and injunctive relief for recovery of economic injury on behalf of Class Members and it expressly is not intended to request any recovery for personal injury and claims related thereto.

83. The joinder of Class Members is impractical and the disposition of their claims in the Class action will provide substantial benefits both to the parties and to the court. The Class Members can be identified through Defendant's records.

FIRST CAUSE OF ACTION

VIOLATION OF THE WIRETAP ACT

18 U.S.C. § 2510 ET SEQ.

84. The Wiretap Act, as amended by the Electronic Communications and Privacy Act of 1986, prohibits the intentional interception of any wire, oral, or electronic communication.

85. Under 18 U.S.C. § 2520(a) there is a private right of action to any person whose wire, oral, or electronic communication is intercepted.

86. Defendant procured the Session Replay Provider to intercept Plaintiff's and Class Members' electronic communications without consent when Plaintiff and Class Members navigated through Defendant's website.

87. Plaintiff and Class Members were unaware Defendant's Session Replay Provider was intercepting their electronic communications and tracking their communications and interactions with Defendant's website.

88. At Defendant's instruction, the Session Replay Provider, intentionally utilized technology – the session replay spyware – as a means of intercepting and acquiring the contents of Plaintiff's and Class Members' electronic communications, in violation of 18 U.S.C. § 2511(1)(a).

89. On information and belief, Defendant disclosed the contents of the electronic communications to third parties, knowing that the information was obtained through the interception of electronic communications thereby violating 18 U.S.C. § 2511(1)(c).

90. Defendant used the contents of the electronic communications for business purposes when it knew that the information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(1)(d).

91. Plaintiff and Class Members are persons whose electronic communications were intercepted by Defendant. As such, they are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of $10,000

or $100 per day for each violation, actual damages, punitive damages, and reasonable attorneys' fees and costs under 18 U.S.C. § 2520.

SECOND CAUSE OF ACTION

VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT

CALIFORNIA PENAL CODE § 631

92. Defendant aided the Provider to tap Plaintiff's and California Class Members' private electronic communications and transmissions when they accessed Defendant's website from within the State of California.

93. Plaintiff and California Class Members did not know Defendant's Provider was engaging in such tapping and therefore could not provide consent to have any part of their private electronic communications tapped.

94. Plaintiff and California Class Members were completely unaware that Defendant had aided the Provider to tap electronic communications until well after the fact and were therefore unable to consent.

95. Neither Defendant, or the Provider, advised Plaintiff or the other California Class Members that any part of their electronic communications with Defendant's website would be tapped.

96. To establish liability under section 631(a), a plaintiff need only establish that a defendant, or its co-conspirator, "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, including the 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 this 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.

97. 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).

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

99. By using the session replay spyware to track, record, and attempt to learn the contents of Plaintiff's and California Class Members' electronic communications, Defendant intentionally aided in the tapping, electrotonically

or otherwise, the lines of internet communication of Plaintiff and California Class Members.

100. By utilizing the session replay spyware, Defendant's co-conspirator willfully and without consent, read or attempted to read or learn the contents or meaning of electronic communications of Plaintiff and putative California Class Members, while the electronic communications were in transit or passing over a wire, line or cable or were being sent from or received at a place in California with the aid of Defendant.

101. Plaintiff and California Class Members did not consent to any of Defendant's, or the Provider's actions, in implementing these unauthorized connections, nor have Plaintiff or California Class Members consented to Defendant's intentional access, interception, reading, learning, recording, and collection of Plaintiff's and California Class Members' electronic communications.

102. Plaintiff's and the California Class Members' devices that Defendant and its co-conspirator accessed through its unauthorized actions included their computers, smart phones, and tablets and/or other electronic computing devices.

103. Defendant aided Provider in tapping, connecting to, intercepting, accessing, taking and using Plaintiff's and the California Class Members' communications in violation of Cal. Penal Code § 631(a).

104. Defendant aided Provider in willfully and without consent reading or learning the contents or meaning of a communication while the same was in transit or passing over a wire, line or cable in violation of Cal. Penal Code § 631(a).

105. Defendant aided Provider in using, or attempting to use, or communicate the information it intercepted in violation of Cal. Penal Code § 631(a).

106. Defendant aided, agreed with, employed, or conspired to unlawfully do, or permit, or caused the unlawful acts above in violation of Cal. Penal Code § 631(a).

///

107. Plaintiff and California Class Members are entitled to statutory damages of $5,000 per violation of Cal. Pen. Code § 631(a) pursuant to Cal. Pen. Code § 637.2(a)(1).

108. Plaintiff's counsel is entitled to attorneys' fees and costs under Cal. Code of Civ. Proc. § 1021.5.

THIRD CAUSE OF ACTION

VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT

CALIFORNIA PENAL CODE § 632

109. Defendant used, or conspired to use, session replay spyware to secretly record the confidential communications of Plaintiff and California Class Members when they visited Defendant's website.

110. Defendant did not warn or advise Plaintiff and California Class Members that it was using, or conspiring to use, session replay spyware to record their communications with its website.

111. Defendant did not obtain consent prior to recording any of their communications.

112. Defendant's conduct violated Cal. Pen. Code § 632(a).

113. Plaintiff and California Class Members are entitled to statutory damages of $5,000 per violation of Cal. Pen. Code § 632(a) pursuant to Cal. Pen. Code § 637.2(a)(1).

114. Plaintiff's counsel is entitled to attorneys' fees and costs under Cal. Code of Civ. Proc. § 1021.5.

FOURTH CAUSE OF ACTION

VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT

CALIFORNIA PENAL CODE § 632.7

115. Defendant used, or conspired to use, session replay spyware to surreptitiously record the communications of Plaintiff and Class Member when they visited Defendant's website via their cell phones.

///

116. Defendant had a policy of not advising or warning Plaintiff and Class Members that it was using session replay spyware to record, or conspire to record, their cellular communications with Defendant's website.

117. Defendant refused to obtain consent of Plaintiff and Class Members prior to the recording of any of their cellular communications.

118. Defendant's conduct violated Cal. Pen. Code § 632.7(a).

119. Plaintiff and Class Members are entitled to statutory damages of $5,000 per violation of Cal. Pen. Code § 632.7(a) pursuant to Cal. Pen. Code § 637.2(a)(1).

120. Plaintiff's counsel is entitled to attorneys' fees and costs under Cal. Code of Civ. Proc. § 1021.5.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class Members pray that judgment be entered against Defendant, and that Plaintiff and Class Members be awarded the following:

- Certify the Classes as requested herein;
- Appoint Plaintiff to serve as the Class Representative for the Classes;
- Appoint Plaintiff's Counsel as Class Counsel in this matter;
- Preliminary and other equitable or declaratory relief as may be appropriate under 18 U.S.C. § 2520(b)(1);
- The greater of $10,000 or $100 per day for each violation of 18 U.S.C. § 2510 et seq pursuant to 18 U.S.C. § 2520(b)(2) and 18 U.S.C. § 2520(c)(2)(B);
- Reasonable attorneys' fees and other litigation costs reasonably incurred pursuant to 18 U.S.C. § 2520(b)(3);
- $5,000 per violation of Cal. Pen. Code §§ 631, 632 and 632.7 to each CIPA Class Member pursuant to Cal. Pen. Code § 637.2(a)(1);
- Reasonable attorneys' fees pursuant to Cal. Code of Civ. Proc. § 1021.5;
- Injunctive relief to prevent the further violations of Cal. Pen. Code §§ 631, 632 and 632.7;
- An award of costs to Plaintiff; and

- Any other relief the Court may deem just and proper including interest.

TRIAL BY JURY

121. Pursuant to the Seventh Amendment to the Constitution of the United States of America, Plaintiff and Class Members are entitled to, and demand, a trial by jury.

Respectfully submitted,

SWIGART LAW GROUP

Date: February 10, 2023

By: *s/ Joshua Swigart*
Joshua B. Swigart, Esq.
Josh@SwigartLawGroup.com
Attorneys for Plaintiff

LAW OFFICE OF DANIEL G. SHAY

Date: February 10, 2023

By: *s/ Daniel Shay*
Daniel G. Shay, Esq.
DanielShay@TCPAFDCPA.com
Attorney for Plaintiff

ClassAction.org
