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

JOAN WRIGHT, individually and on behalf of others similarly situated, Plaintiff, vs. ULTA SALON, COSMETICS & FRAGRANCE, INC., Defendant.	CASE NO: **'22CV1954 BAS BLM** 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 JURY TRIAL DEMANDED

INTRODUCTION

1. Joan Wright ("Plaintiff"), individually and on behalf of all other similarly situated consumers ("Class Members"), brings this action for damages and injunctive relief against Ulta Salon, Cosmetics & Fragrance, 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, 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 taping or interception of any wire, oral, or electronic communication. In addition to other relevant sections, the Wire Tap Act states that any person that;

> "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).

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 read, learn the contents of, and make reports on Plaintiff's and Class Members' interactions on Defendant's website.

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 which provides for statutory damages of $2,500 for each violation, pursuant to California Penal Code § 631(a).

7. As discussed in detail below, Defendant utilized "session replay" spyware to intercept Plaintiff's and the Class Members' electronic computer-to-computer data communications, including how Plaintiff and Class Members interacted with the website, mouse movements and clicks, keystrokes, search items, 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 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.*, what Plaintiff and Class Members searched for, looked at, the information inputted, and clicked on.

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

///

///

///

9. The "session replay" spyware utilized by Defendant is a sophisticated computer software that allows Defendant to contemporaneously intercept, capture, read, observe, re-route, forward, redirect, and receive Plaintiff's and Class Members' electronic communications.

10. "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)).

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

12. 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 when visiting Defendant's website. The

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

technology also permits companies like Defendant to view the interactions of visitors on Defendant's website in live, real-time.

13. The purported use of "session replay" technology is to monitor and discover broken website features; however, the extent and detail collected by users of the technology, like Defendant, far exceeds the stated purpose and 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 a website, but also allows the user to create a detailed profile for each visitor to the site.

14. Moreover, the collection and storage of page content may cause sensitive information and other personal information displayed on a page to lead to third parties. This may expose website visitors to identity theft, online scams, and other unwanted behavior.

15. 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]

16. 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:

(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/;

///

///

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

(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

17. In sum, Defendant illegally tapped, made an unauthorized connection to, and intercepted Plaintiff's and Class Members' electronic communications through visits to Defendant's website, causing injuries, including violations of Plaintiff's and Class Members' substantive legal privacy rights under the Wiretap Act and CIPA.

18. 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.

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

///

///

///

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

21. Unless otherwise indicated, 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

22. Plaintiff is a natural person and resident of the State of California and the County of San Diego.

23. Defendant is a Delaware entity with its principal place of business located in Illinois.

24. 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

25. Jurisdiction of this Court is proper pursuant to 28 U.S.C. § 1331 because this action arises out of Defendants' violations of the Wiretap Act, 18 U.S.C. §2510 et seq.

26. Jurisdiction is also established 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) a California subclass, which will result in at least one Class Member belonging to a different state than Defendant, a Delaware entity with its principal place of business in Illinois.

27. 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 $2,500 per violation of Cal. Penal Code §631, 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.

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

29. Because Defendant conducts business within the State of California, personal jurisdiction is established.

30. 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

31. Defendant owns and operates the following website: www.ulta.com.

32. Over the last few years, Plaintiff and Class Members visited Defendant's website and were in California at the time.

33. During visits to the website, Plaintiff and Class Members, through computers and mobile devices, transmitted electronic communications in the form of instructions to Defendant's computer servers utilized to operate the website. The commands were sent as messages indicating to Defendant what content was being viewed, clicked on, requested and/or inputted by Plaintiff and Class Members.

34. The communications sent by Plaintiff and Class Members to Defendant's servers included the following actions taken by Plaintiff and Class Members while on Defendant's website: mouse clicks and movements, keystrokes, search items, information inputted by Plaintiff and Class Members, pages and content viewed by Plaintiff and Class Members, scroll movements, and copy and paste actions.

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

///

36. Plaintiff and Class Members reasonably expected that visits to Defendant's website would be private, and that Defendant would not be intercepting or tapping 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.

37. 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 worse yet, monitored live while Plaintiff and Class Members were on its website.

38. Upon information and belief, over the last few years, Defendant has had embedded within its website code and has continuously operated at least one "session replay" script that was provided by a third party ("Session Replay Provider"). The "session replay" spyware was always active and intercepted every incoming data communication to Defendant's website the moment a visitor accessed the site.

39. The Session Replay Provider that provided that "session replay" spyware to Defendant is not a provider of wire or electronic communication services, or an internet service provider.

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

41. 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 to its websites, and the information collected was solely for Defendant's own benefit.

///

42. 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.

43. During one or more of Plaintiff's and Class Members' visits to Defendant's website, Defendant utilized "session replay" spyware to intercept the substance of Plaintiff's and Class Members' electronic communications intentionally and contemporaneously with Defendant's website, including mouse clicks and movements, keystrokes, search terms, information inputted 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.

44. 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.

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

46. 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 Member's internet activity and habits.

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

///

///

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

49. The "session replay" spyware utilized by Defendant intercepted, tapped and made unauthorized connections, which allowed Defendant to learn the contents of communications of Plaintiff and Class Members in a manner that was undetectable to them.

50. Defendant then stored the communications and played them back and analyzed them for business purposes.

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

52. 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 or seek consent from Plaintiff or Class Members prior to making the connections to the electronic communications through the "session replay" spyware.

STANDING

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

54. 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

55. 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

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

57. Plaintiff proposes the following Class and Subclass, consisting of and defined as follows:

> Class
> All persons in the United States whose communications were intercepted by Defendant or its agents.
>
> Subclass
> All persons in California whose communications were intercepted by Defendant or its agents.

///

///

///

58. 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.

59. **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.

60. **Commonality**: There are common questions of law and fact as to Class Members that predominate over questions affecting only individual members, including:

- 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 Plaintiff and Class Members were aware of Defendant's "session replay" spyware and had consented to its use.

61. **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.

62. 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.

63. **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.

///

///

64. **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.

65. **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.

66. 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.

67. 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.

68. 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.

69. 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.

70. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs of this complaint.

71. 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.

72. 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.

73. Defendant intercepted Plaintiff's and Class Members' electronic communications without consent when Plaintiff and Class Members navigated through Defendant's website.

74. Plaintiff and Class Members were unaware Defendant was intercepting their electronic communications and tracking their communications and interactions with Defendant's website.

75. Defendant 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.

76. 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

UNLAWFUL WIRETAPPING AND INTERCEPTION OF ELECTRONIC COMMUNICATION

CALIFORNIA PENAL CODE § 631

77. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs of this complaint.

78. Defendant intercepted components of Plaintiff's and Class Members' private electronic communications and transmissions when Plaintiff and other Class Members accessed Defendant's website from within the State of California.

///

79. Plaintiff and Class Members did not know Defendant was engaging in such interception and therefore could not provide consent to have any part of their private electronic communications intercepted by Defendant.

80. Plaintiff and Class Members were completely unaware that Defendant had intercepted and stored electronic communications and other personal data until well after the fact and were therefore unable to consent.

81. Defendant never advised Plaintiff or the other Class Members that any part of this communications or their use of Defendant's website would be tapped.

82. 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, 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.

83. 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).

84. Defendant'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.

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

86. By utilizing the "session replay" spyware, Defendant willfully and without consent, read or attempted to read or learn the contents or meaning of electronic communications of Plaintiff and putative 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.

87. Plaintiff and Class Members did not consent to any of Defendant's actions in implementing these unauthorized connections, nor have Plaintiff or Class Members consented to Defendants' intentional access, interception, reading,

learning, recording, and collection of Plaintiff's and Class Members' electronic communications.

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

89. Defendant violated Cal. Penal Code § 631 by knowingly accessing, and without permission accessing, Plaintiff's and Class Members' electronic communications through the use of the "session replay" spyware in order for Defendant to track, understand, and attempt to learn the contents of Plaintiff's and Class Members' electronic communications generated by the use of Defendant's website.

90. Defendant violated Cal. Penal Code § 631 by knowingly and without permission intercepting, wiretapping, accessing, taking and using Plaintiff's and the Class Members' communications.

91. Plaintiff and Class Members seek relief available under Cal. Penal Code § 631, including $2,500 per violation.

PRAYER FOR RELIEF

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

- Certify the Class and Subclass;
- Appoint Plaintiff to serve as the Class Representative for the Class and Subclass;
- Appoint Plaintiff's Counsel as Class Counsel;
- Preliminary and other equitable or declaratory relief 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 costs pursuant to 18 U.S.C. § 2520(b)(3);
- $2,500 to each Subclass Member pursuant to California Penal Code § 631(a).

///

- Reasonable attorneys' fees and costs pursuant to Cal. Code of Civ. Proc. § 1021.5;
- Injunctive relief to prevent the further violations of California Penal Code § 631.
- An award of costs to Plaintiff; and
- Any other relief the Court may deem just and proper including interest.

TRIAL BY JURY

92. 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: December 9, 2022

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

LAW OFFICE OF DANIEL G. SHAY

Date: December 9, 2022

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

ClassAction.org
