IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

JOHN JACOBO III, individually and on behalf of all others similarly situated, Plaintiff, v. FOOT LOCKER RETAIL, INC. and SESSIONCAM LTD, Defendants.	Civil Action No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff John Jacobo III ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his attorneys, makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to allegations specifically pertaining to himself and his counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action suit brought against Defendants Foot Locker Retail, Inc. ("Foot Locker") and SessionCam Ltd ("SessionCam") (collectively, "Defendants") for wiretapping the electronic communications of visitors to Defendant Foot Locker's website, footlocker.com (the "Website"). The wiretaps, which are embedded in the computer code on the Website, are used by Defendants to secretly observe and record website visitors' keystrokes, mouse clicks,[1] and other electronic communications, including the entry of Personally Identifiable Information ("PII"), in real time. By doing so, Defendants have violated the

[1] As used herein, the term "mouse clicks" also refers to "touch gestures" such as the "tap," "swipe," and similar gestures used on touchscreen devices.

California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 631 and 635, and invaded Plaintiff's and Class Members' privacy rights in violation of the California Constitution.

2. In December 2020, Mr. Jacobo III visited the Website. During the visit, Defendants recorded Plaintiff's electronic communications in real time, including Plaintiff's mouse clicks, keystrokes, and payment card information.

3. Plaintiff brings this action on behalf of himself and a class of all persons in the state of California whose electronic communications were intercepted through the use of Defendants' wiretap on the Website.

THE PARTIES

4. Plaintiff John Jacobo III is a California citizen and resident who lives in Fresno, California. Mr. Jacobo III is domiciled and intends to remain in California. In December 2020, prior to the filing of this lawsuit, Mr. Jacobo III visited the Website and purchased sneakers from the Website. Mr. Jacobo III was in California when he visited the website. During the visit, Mr. Jacobo III's keystrokes, mouse clicks, and other electronic communications—including the entry of his payment card information—were intercepted in real time and were disclosed to Defendants Foot Locker and SessionCam through the wiretap. Mr. Jacobo III was unaware at the time that his keystrokes, mouse clicks, and other electronic communications, including the information described above, were being intercepted in real-time and would be disclosed to SessionCam, nor did Mr. Jacobo III consent to the same.

5. Defendant Foot Locker Retail, Inc. is a company incorporated under the laws of New York with its principal place of business at 330 West 34th Street, New York, New York 10001. Defendant operates the Website from its place of business in New York City.

6. Foot Locker does business throughout California and the entire United States.

7. Foot Locker owns and operates the Website.

8. Defendant SessionCam Ltd is an English corporation with its principal place of business at St. Vedast House, St. Vedast Street, Norwich, NR1 1BT, England.

9. SessionCam is a marketing software-as-a-service ("SaaS") company.

10. SessionCam provides a feature called "Session Replay," which is at issue here and described more fully below. At all relevant times herein, Foot Locker has used SessionCam's "Session Replay" product on the Website and Defendants have conspired together to violate Class Members' privacy.

JURISDICTION AND VENUE

11. 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, and at least one member of the proposed class is citizen of state different from at least one Defendant.

12. This Court has personal jurisdiction over Defendants because each of the Defendants have purposefully availed themselves of the laws and benefits of doing business in this State, and Plaintiff's claims arise out of each of the Defendants' forum-related activities. Furthermore, a substantial portion of the events giving rise to Plaintiff's claims occurred in this District. In addition, Defendant Foot Locker is incorporated and headquartered in this District.

13. 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 and Defendant Foot Locker resides in this District. Further, Defendant SessionCam, as a foreign corporation, may be sued in any judicial district.

STATEMENT OF FACTS

I. Overview Of The Wiretaps

14. Defendant SessionCam develops a software of the same name that provides marketing analytics.

15. One of SessionCam's features is called "Session Replay."

16. SessionCam tells prospective clients that they can "[u]se session replay to see the website experience you actually deliver to your customers across desktop, mobile and tablet devices."

17. Session Replay "records an exact version of the page as seen by the user at the time of use; including the HTML, CSS and all images." The recording allows companies to "see mouse movements, clicks/taps, masked form input, page scrolling and mobile gestures like pinch, zoom, tap, double tap, swipe, tilt and screen resizing."

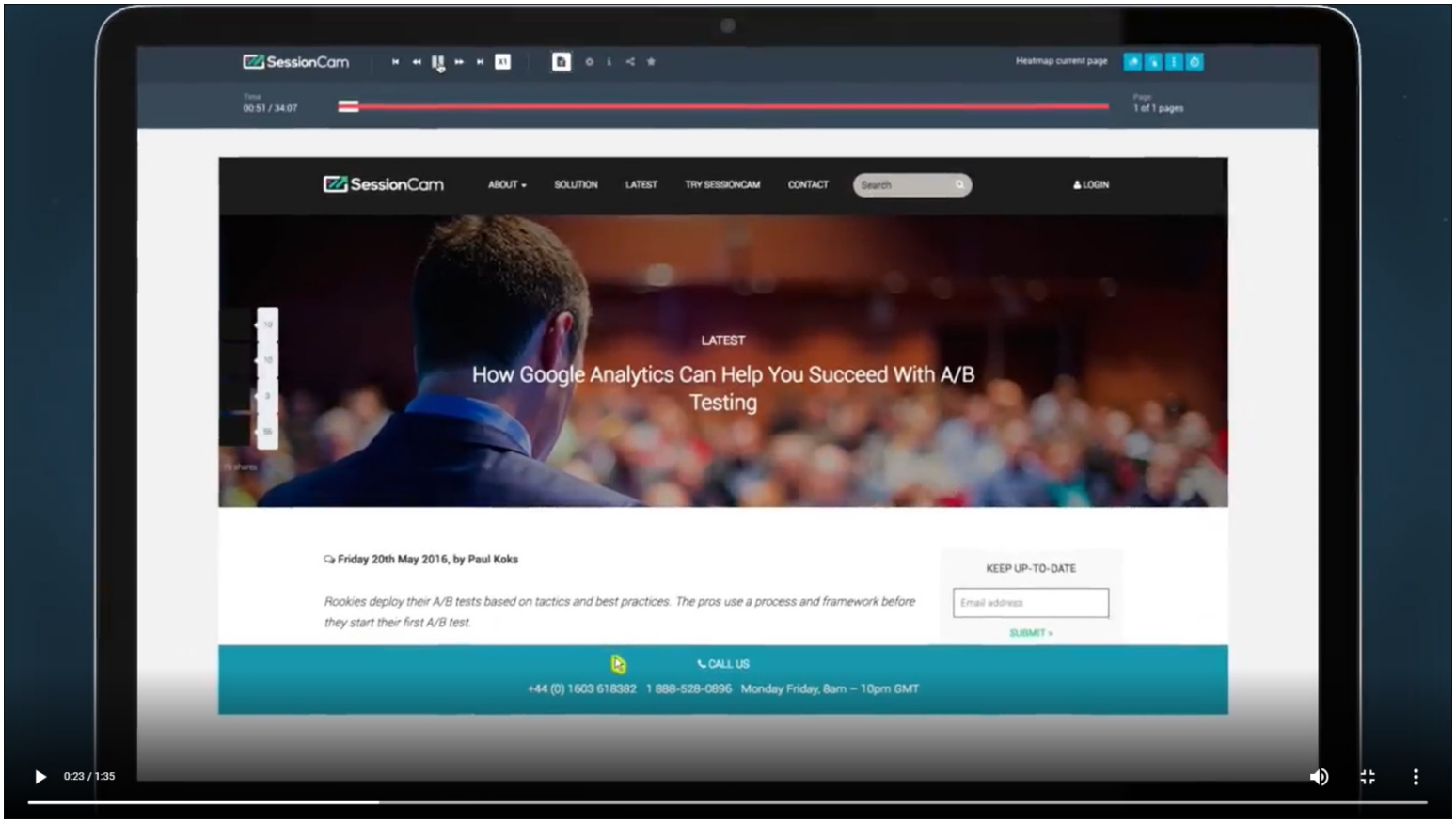
18. Session replay technologies work by using "embedded snippets of code … [that] watch and record a visitor's every move on a website, in real time."[2]

19. SessionCam's code is not a cookie at all, much less a run-of-the-mill cookie. Common cookies that consumers might be familiar with do not engage in session recording or all of the features described above. SessionCam's code does far more than simply track where a visitor went on the internet, and its functionality is not limited to aggregate data. Rather, as a 2017 study by Princeton University researchers—which specifically examined SessionCam—noted, "unlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions, as if someone is

[2] Tomas Foltyn, *What's the Deal with Session-Replay Scripts?*, WELIVESECURITY, Apr. 20, 2018, https://www.welivesecurity.com/2018/04/20/whats-deal-session-replay-scripts/.

looking over your shoulder."

20. Indeed, SessionCam's promotional video touts that Session Replay "let[s] you record live user sessions, looking over the shoulder of your real-life customers." The highlighted mouse in the promotion video shows the Session Replay software tracking a mock user's mouse movements in real-time:



21. Technology like SessionCam's Session Replay feature is not only highly intrusive, but dangerous. A 2017 study by Princeton University found that session recording technologies were collecting sensitive user information such as passwords and credit card numbers. The research notes that this was not simply the result of a bug, but rather insecure practices. Thus, session recording technologies such as SessionCam's can leave users vulnerable to data leaks and the harm resulting therefrom.

22. SessionCam's business model involves entering into voluntary partnerships with various companies and providing their software to their partners.

23. One of SessionCam's partners is Defendant Foot Locker.

24. Foot Locker utilizes SessionCam's software on the Website.

25. Foot Locker knows that SessionCam's software captures the keystrokes, mouse clicks and other communications of visitors to its website, and pays SessionCam to supply that information.

26. Pursuant to an agreement with SessionCam, Foot Locker enables SessionCam's software by voluntarily embedding SessionCam's software code on the Website.

27. As currently deployed, SessionCam's software, as employed by Foot Locker, functions as a wiretap.

II. Defendants Wiretapped Plaintiff's Electronic Communications

28. In December 2020, Mr. Jacobo III visited Foot Locker.com and made a purchase.

29. During that visit, and upon information and belief, the Session Replay feature in SessionCam's software created a video capturing each of Plaintiff's keystrokes and mouse clicks on the website. The SessionCam wiretap also captured the date and time of the visit, the duration of the visit, Plaintiff's IP address, his location at the time of the visit, his browser type, and the operating system on his device.

30. SessionCam's recording of keystrokes, mouse clicks, data entry, and other electronic communications begins the moment a user accesses or interacts with the Website.

31. When users access the Website and make a purchase, they enter their PII. SessionCam's software captures these electronic communications throughout each step of the process. Even if a user does not make a purchase, the SessionCam nonetheless captures users' electronic communications throughout his or her visit on the Website.

32. SessionCam's software captures, among other things:

(a) The user's mouse clicks;

(b) The user's keystrokes;

(c) The user's payment card information, including card number, expiration date, and CVV code;

(d) The user's IP address;

(e) The user's their location at the time of the visit; and

(f) The user's browser type and the operating system on their devices

33. Crucially, Defendant Foot Locker does not ask users, including Plaintiff, whether they consent to being wiretapped by SessionCam. Users are never actively told that their electronic communications are being wiretapped by SessionCam.

34. Further, as the 2017 Princeton University study researchers recognized, "the extent of data collected by these services **far exceeds user expectations**; text typed into forms is collected before the user submits the form, and precise mouse movements are saved, all without any visual indication to the user. This data can't reasonably be expected to be kept anonymous."

35. Therefore, users like Plaintiff never consent to being wiretapped by SessionCam when they access the Website.

CLASS ACTION ALLEGATIONS

36. Plaintiff seeks to represent a class of all California residents who visited the

Website, and whose electronic communications were intercepted or recorded by SessionCam. Plaintiff reserves the right to modify the class definition as appropriate based on further investigation and discovery obtained in the case.

37. Members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in the thousands. The precise number of Class members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendants.

38. Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to, whether Defendants have violated the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 631 and 635, and invaded Plaintiff's privacy rights in violation of the California Constitution; and whether class members are entitled to actual and/or statutory damages for the aforementioned violations.

39. The claims of the named Plaintiff are typical of the claims of the Class because the named Plaintiff, like all other class members, visited the Website and had his electronic communications intercepted and disclosed to SessionCam through the use of SessionCam's wiretaps.

40. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class members he seeks to represent, he has retained competent counsel experienced in prosecuting class actions, and he intends to prosecute this action vigorously. The interests of Class members will be fairly and adequately protected by Plaintiff and his counsel.

41. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class members. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendants' liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendants' liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

42. Plaintiff brings all claims in this action individually and on behalf of members of the Class against Defendants.

COUNT I
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 631

43. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

44. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendants.

45. To establish liability under section 631(a), Plaintiff need only establish that Defendants, "by means of any machine, instrument, contrivance, or in any other manner," did 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.

46. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *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*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history).

47. SessionCam's software, including its Session Replay feature, is a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

48. At all relevant times, by using SessionCam's technology, Defendants intentionally tapped, electrically or otherwise, the lines of internet communication between Plaintiff and Class Members on the one hand, and Foot Locker's Website on the other hand.

49. At all relevant times, by using SessionCam's technology, Defendants willfully and without the consent of all parties to the communication, or in any unauthorized manner, 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 any wire, line or cable or were being sent from or received at any place within California.

50. As SessionCam notes on its website, "When an end user session is recorded by the SessionCam script, SessionCam starts by recording event data locally in the browser. Every few seconds, this local event data is packaged up and sent to SessionCam recording servers in the form of bundles." Such local recording is plainly occurring in real-time, and is, at worst, "transitory electronic storage" that is "part of the overall transmission process," which has been held to constitute communications "in transit."

51. Indeed, SessionCam offers website operators the ability to "Go Live" with currently active website sessions (*i.e.*, users still have the website open on their browser), which would not be possible if SessionCam was not recording users in real time.

52. Defendants aided, agreed with, and conspired with each other to implement SessionCam's technology and to accomplish the wrongful conduct at issue here. In addition, Foot Locker employed SessionCam to accomplish the wrongful conduct at issue here.

53. Plaintiff and Class Members did not consent to any of Defendants' actions in implementing SessionCam's wiretaps on the Website. Nor have Plaintiff nor Class Members

consented to Defendants' intentional access, interception, reading, learning, recording, and collection of Plaintiff and Class Members' electronic communications.

54. The violation of section 631(a) constitutes an invasion of privacy sufficient to confer Article III standing.

55. Unless enjoined, Defendants will continue to commit the illegal acts alleged here. Plaintiff continues to be at risk because he frequently uses the internet for shopping, and he continues to desire to use the internet for that purpose. Defendant SessionCam provides its software, including the Session Replay feature, to many other website operators who offer a wide array of services. For many websites that Plaintiff may or is likely to visit in the future, he has no practical way to know if his website communications will be monitored or recorded by SessionCam.

56. Plaintiff and Class Members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of $5,000 per violation.

COUNT II
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 635

57. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

58. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

59. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendants.

60. California Penal Code § 635 provides, in pertinent part:

> Every person who manufactures, assembles, sells, offers for sale, advertises for sale, possesses, transports, imports, or furnishes to

> another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another, or any device which is primarily or exclusively designed or intended for the unauthorized interception or reception of communications between cellular radio telephones or between a cellular radio telephone and a landline telephone in violation of Section 632.5, or communications between cordless telephones or between a cordless telephone and a landline telephone in violation of Section 632.6 , shall be punished by a fine not exceeding two thousand five hundred dollars.

61. At all relevant times, by implementing SessionCam's wiretaps, each Defendant intentionally manufactured, assembled, sold, offered for sale, advertised for sale, possessed, transported, imported, and/or furnished a wiretap device that is primarily or exclusively designed or intended for eavesdropping upon the communication of another.

62. SessionCam's code is a "device" that is "primarily or exclusively designed" for eavesdropping. That is, the SessionCam's code is designed to gather PII, including keystrokes, mouse clicks, and other electronic communications.

63. Plaintiff and Class Members did not consent to any of Defendants' actions in implementing SessionCam's wiretaps.

64. Unless enjoined, Defendants will continue to commit the illegal acts alleged here. Plaintiff continues to be at risk because he frequently uses the internet for shopping, and he continues to desire to use the internet for that purpose. Defendant SessionCam provides its software, including the Session Replay feature, to many other website operators who offer a wide array of services. For many websites that Plaintiff may or is likely to visit in the future, he has no practical way to know if his website communications will be monitored or recorded by SessionCam.

65. Plaintiff and Class Members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of $5,000 per violation.

COUNT III
Invasion Of Privacy Under California's Constitution

66. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

67. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

68. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendants.

69. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential PII; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various Internet sites without being subjected to wiretaps without Plaintiff's and Class Members' knowledge or consent.

70. At all relevant times, by implementing SessionCam's wiretaps on Foot Locker's Websites, each Defendant intentionally invaded Plaintiff's and Class Members' privacy rights under the California Constitution, and procured the other Defendant to do so.

71. Plaintiff and Class Members had a reasonable expectation that their PII and other data would remain confidential and that Defendants would not install wiretaps on the Website.

72. Plaintiff and Class Members did not consent to any of Defendants' actions in implementing SessionCam's wiretaps on the Website.

73. This invasion of privacy is serious in nature, scope and impact.

74. This invasion of privacy alleged here constitutes an egregious breach of the social norms underlying the privacy right.

75. Plaintiff and Class Members seek all relief available for invasion of privacy claims under California's Constitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendants, as follows:

(a) For an order certifying the Class under Rule 23 and naming Plaintiff as the representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order declaring that the Defendants' conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For compensatory, punitive, and statutory damages in amounts to be determined by the Court and/or jury;

(e) For prejudgment interest on all amounts awarded;

(f) For an order of restitution and all other forms of equitable monetary relief;

(g) For injunctive relief as pleaded or as the Court may deem proper; and

(h) For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit.

DEMAND FOR TRIAL BY JURY

Pursuant to Federal Rules of Civil Procedure 38(b), Plaintiff demands a trial by jury of all issues so triable.

Dated: January 19, 2021

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Yitzchak Kopel*
Yitzchak Kopel

Yitzchak Kopel
Philip L. Fraietta
Max S. Roberts
888 Seventh Avenue, Third Floor
New York, New York 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: ykopel@bursor.com
pfraietta@bursor.com
mroberts@bursor.com

Attorneys for Plaintiff