COMMONWEALTH OF PENNSYLVANIA
COURT OF COMMON PLEAS
COUNTY OF CUMBERLAND
9TH JUDICIAL CIRCUIT

MATTHEW FARST, *individually and on behalf of all others similarly situated,* Plaintiff, v. AUTOZONE, INC. and AUTOZONE.COM, INC., Defendant.	Case No. 2024-00002 **CLASS ACTION** **JURY TRIAL DEMANDED**

AMENDED CLASS ACTION COMPLAINT

Plaintiff Matthew Farst brings this class action against Defendant Autozone, Inc. and Autozone.com, Inc. (collectively "Defendants" or "Autozones") and alleges as follows upon personal knowledge as to Plaintiff and Plaintiff's own acts and experiences, and, as to all other matters, upon information and belief, including investigation on conducted by Plaintiff's attorneys.

NATURE OF THE ACTION

1. "Since the advent of online behavioral advertising ('OBA') in the late 1990s, businesses have become increasingly adept at tracking users visiting their websites." *Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d 108, 111 (W.D. Pa. 2019) (citations omitted). This case involves one of the most egregious examples of such consumer tracking and Internet privacy violations.

2. Plaintiff brings this case as a class action under the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. 5701, *et seq.* ("WESCA"). The case stems from Defendants' unlawful procurement of the interception of Plaintiff's and Class members'

electronic communications through the use of third party "session replay" spyware that allowed an undisclosed party record Plaintiff's and the Class members' visits to its website.

3. A recent paper addressed the growing concern held by consumers regarding their digital privacy, indicating how most website visitors will assume their detailed interactions with a website will only be used by that website host and not be shared with any unknown third parties.[1] As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[2] According to a study by the Pew Research Center, a majority of Americans are concerned about how data is collected about them by companies.[3] These concerns are evident by user actions consistent with that expectation of privacy. For example, following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[4]

4. As discussed in detail below, ignored these concerns and procured and utilized "session replay" spyware from third party Session Replay Providers, namely Tealeaf, Quantum Metric and Glassbox, who contemporaneously intercepted Plaintiff's and the Class members' electronic computer-to-computer data communications with Defendants' website, including how

---

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

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

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

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

they interacted with the websites, their mouse movements and clicks, keystrokes, search terms, descriptive URLS, information and PII inputted into the website, their device, their browser, their location, unique identifiers IDs, their internet service provider and pages and content viewed while visiting the websites. Defendant facilitated a third party's interception, recording, processing and storage of electronic communications created through the webpages visited by Plaintiff and the Class members, as well as everything Plaintiff and the Class members did on those pages, *e.g.*, what they searched for, what they looked at, the information and personal details that they inputted, and what they clicked on.

5. Defendant knowingly and intentionally procured undisclosed third parties to intercept the electronic communications at issue without the knowledge or prior consent of Plaintiff or the Class members. Defendant did so for its own financial gain and in violation of Plaintiff's and the Class members' rights to be free of intrusion upon their private affairs and to control information concerning their person under the WESCA.

6. The third party "session replay" spyware procured and utilized by Defendant is not a traditional website cookie, tag, web beacon, or analytics tool. It is a sophisticated computer software that allows the Session Replay Provider to contemporaneously intercept, capture, read, observe, re-route, forward, redirect, and receive incoming electronic communications to Defendants' websites. Plaintiff's and the Class members' electronic communications are then interpreted, reproduced, and stored at Defendants' behest using outside vendor(s)'s services and can later be viewed and utilized by Defendant as a session replay, which is essentially a video of a Class member's entire visit to Defendants' websites, including all of their actions.

7. "Technological advances[,]" such as Defendants' use of session replay technology, "provide 'access to a category of information otherwise unknowable' and 'implicate

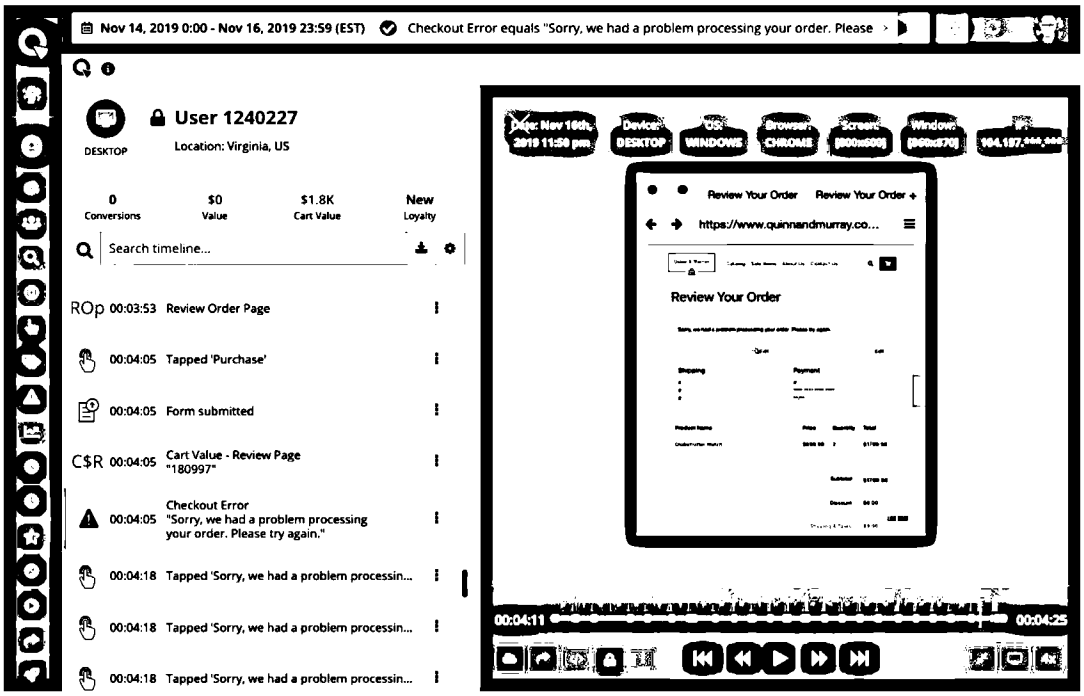
privacy concerns' in a manner different from traditional intrusions as a 'ride on horseback' is different from 'a flight to the moon.'" *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019) (quoting *Riley v. California*, 573 U.S. 373, 393 (2014)).

8. The CEO of a major "session replay" software company – while discussing the merger of his company with another "session replay" provider – publicly exposed why companies like Defendant engage in recording visitors 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[.]" *See Contentsquare Acquires Clicktale to Create the Definite Global Leader in Experience Analytics*, available at www.prnewswire.com/news-releases/contentsquare-acquires-clicktale-to-create-the-definitive-global-leader-in-experience-analytics-300878232.html (last accessed May 10, 2021) (emphasis supplied). This CEO further admitted 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 customers and partners, ***we are accelerating the interpretation of human behavior online and shaping a future of addictive customer experiences***." *Id.* (emphasis supplied).

9. Unlike typical website analytics services that provide aggregate statistics, the third party session replay technology utilized by Defendant is intended to record and capture electronic communications on Defendants' websites and then process those communications to create a playback of individual browsing sessions, something akin to as if someone is looking over a Class members' shoulder when visiting Defendants' websites. The technology also permits companies like Defendant to view the interactions of visitors on their websites in real-time.

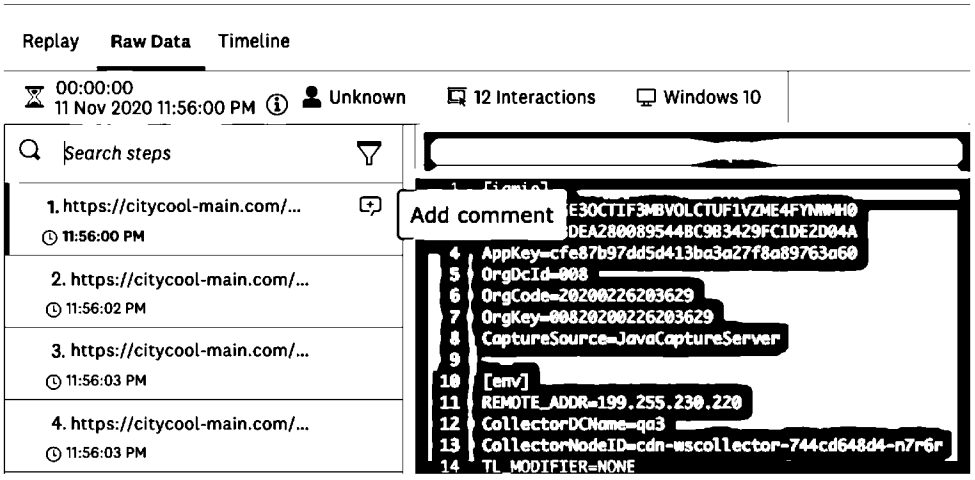
10. The following screenshots provide an example of a typical recording of a visit to a website captured utilizing session replay software, which includes mouse movements, keystrokes and clicks, search terms, content viewed, and information inputted by the website visitor:

Quantum Metric:



Glassbox:

Tealeaf:



11. The purported use of session replay technology is to monitor and discover broken website features. However, the extent and detail of the data collected by the Session Replay Providers for users of the technology, such as Defendant, far exceeds the stated purpose and Plaintiff's and the Class members' reasonable expectations when visiting websites like

Defendants'. The technology not only allows the recording and viewing of a visitor's detailed electronic communications with a website, but also allows the user (and the Session Replay Provider) to create a detailed profile for each visitor to the site. Indeed, in an ongoing patent dispute, a well-known session replay provider openly admitted that this type of technology is utilized by companies like Defendant to make a profit: **"[the] software computes billions of touch and mouse movements and transforms this knowledge into profitable actions that increase engagement, reduce operational costs, and maximize conversion rates (i.e., the percentage of users who take desired actions on a website, such as purchasing a product offered for sale)**." *Content Square SAS v. Quantum Metric, Inc.,* Case No. 1:20-cv-00832-LPS, Compl. at ¶8, [DE 1] (D. Del. Jun. 22, 2020) (emphasis supplied).

12. Moreover, the collection and storage of page content creates a material risk that sensitive information and other personal identifying information displayed on a page will leak to additional third parties. This may expose website visitors to identity theft, online scams, and other unwanted behavior.

13. In 2019, Apple warned application developers using session replay technology that they were required to disclose such tracking and recording 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." https://techcrunch.com/2019/02/07/apple-glassbox-apps/ (last visited November 22, 2023).

14. 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 the following examples:

(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/ (last visited November 22, 2023);

(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/ (last visited November 22, 2023);

(c) ***Are Session Recording Tools a Risk to Internet Privacy?***, located at https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/ (last visited November 22, 2023);

(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 (last visited November 22, 2023);

(e) ***Session Replay Scripts Could be Leaking Sensitive Data***, located at https://medium.com/searchencrypt/session-replay-scripts-could-be-leaking-sensitive-data-5433364b2161 (last visited November 22, 2023);

(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 (last visited November 22, 2023); and

(g) ***Sites Using Session Replay Scripts Leak Sensitive User Data***, located at https://www.helpnetsecurity.com/2017/11/20/session-replay-data-leak (last visited November 22, 2023).

15. In sum, Defendant procured the interception of the electronic communications of Plaintiff and the Class members through their visits to its websites, causing them injuries, including

violations of their substantive legal privacy rights under the WESCA, invasion of their privacy, intrusion upon their private affairs, and interference with their right to control, and potential additional exposure of, their private information.

16. Through this action, Plaintiff seeks damages authorized by the WESCA on behalf of herself and the Class members, defined below, and any other available legal or equitable remedies to which they are entitled.

PARTIES

17. Plaintiff is, and at all times relevant hereto was, a natural person and a permanent resident of the State of Pennsylvania.

18. Defendant Autozone, Inc. ("Autozone") is, and at all times relevant hereto was, a corporation duly organized and validly existing under the laws of Nevada and maintains its principal place of business in Tennessee. Defendant is therefore a citizen of Nevada and Tennessee. Autozone, Inc. is registered to do business in the Commonwealth of Pennsylvania.

19. Defendant Autozone.com, Inc. ("Autozone.com") is, and at all times relevant hereto was, a corporation duly organized and validly existing under the laws of Virginia and maintains its principal place of business in Tennessee. Defendant is therefore a citizen of Virginia and Tennessee. Autozone.com is a wholly owned subsidiary of Autozone, Inc. and is maintained at the same corporate headquarters and under direction of the same corporate officers as Autozone, Inc.

JURISDICTION AND VENUE

20. This Court has personal jurisdiction over Defendants under Pennsylvania's long arm statute. Pa. Const. Stat.§ 5322.

21. First, Defendant Autozone is registered to do business in the Commonwealth of Pennsylvania. *See* Exhibit A. Pursuant to 15 Pa. Cons. Stat. § 411, and 42 Pa. Cons. Stat. § 5301(a)(2)(i), Defendant Autozone is thus subject to general personal jurisdiction in Pennsylvania. *See Mallory v. Norfolk S. Ry.*, 600 U.S. 122, 143 S. Ct. 2028 (2023). Moreover, Autozone.com is a wholly-owned subsidiary of Autozone and is subject to the same corporate governance and operates as a mere instrumentality which feeds its parents' brick-and-mortar operations, such that Autozone.com is nothing but an alter-ego of Autozone, and is thereby subject to Autozone's general jurisdiction in this state.[5] This is evident even in Autozone's own SEC filings, which draw no distinction between its retail store operations and website operations as its primary business. *See e.g.* Exhibit B, pgs. 4, 6, 8, 11, 27. (e.g. "In addition to our in-store offerings, we sell automotive hard parts, maintenance items, accessories and non-automotive parts through www.autozone.com, for pick-up in store or to be shipped directly to a customer's home or business, with next day or same day delivery programs in most of our U.S. market."; "Our primary website is www.autozone.com."). In fact, Defendant Autozone expressly computes its Results of Operations financial balance sheet by including sales through Autozone.com, including direct-to-home sales, and acknowledges its website sales represent a segment encompassed by its auto parts stores segment. *Id.* at 29-30, 74.

[5] See *Fulano v. Fanjul Corp.*, 2020 PA Super 166, 236 A.3d 1, "[T]here is Pennsylvania precedent for an alter ego theory of personal jurisdiction over a foreign corporation. Generally, a corporate parent will retain its distinct identity and not be subject to the jurisdictions of its subsidiaries, even when it shares common directors, officers and shareholders. However, there is a well recognized exception to these general rules if the record demonstrates that the subsidiary is the alter ego of the parent to the extent that domination and control by the parent corporation renders the subsidiary a mere instrumentality of the parent; under such extreme circumstances the parent corporation may be held to be doing business within the state under the facade of the subsidiary. Personal jurisdiction established where defendants purposely avail themselves of benefits and protections of Pennsylvania law and substantially conduct recurring business affairs through operations of their industrial subsidiaries."

22. Defendant Autozone.com is further subject to specific jurisdiction under 42. Pa.C.S. § 5322(3) & (4), as Plaintiff alleges in his Complaint that Autozone.com caused him harm and tortious injury by an act or omission (namely illegal wiretapping) in and/or outside this Commonwealth.

23. Jurisdiction over Defendants does not violate Due Process because Defendants maintain sufficient minimum contacts with this forum such that it does not offend traditional notions of fair play and substantial justice. Defendants specifically direct, market, and provide their business activities throughout the State of Pennsylvania, and make their active commercial website, including Pennsylvania specific material, targeted to and available to residents of Pennsylvania, including entering into thousands of contracts over the Internet between Pennsylvania residents and Defendants. Upon information and belief, Defendants spend significant funds advertising their services in Pennsylvania and driving Pennsylvania consumers to their website, including using the website to direct consumers to Autozone's ***228*** physical retail locations in the State and providing Pennsylvania specific pricing, offerings, and advertisements via the website. *See* https://www.autozone.com/locations/pa.html. During the relevant time frame, Defendants solicited and entered into contracts for the sale of goods and services with residents of Pennsylvania, including those facilitated through the website that directly related to the Pennsylvania and their Pennsylvania locations, such as their tool rental options and in-store delivery and pickup (*see e.g.* Exhibits C), which involved the knowing and repeated transmission of computer data over the Internet. This resulted in Defendants generating extensive revenue from sales to residents of Pennsylvania via the website, as well accepting payments from Pennsylvania residents through the website and ultimately shipping products to Pennsylvania and directing sales to their physical locations in Pennsylvania. Plaintiff's and the Class members' claims arise directly

from Defendants' operation of the website, its targeting of Pennsylvania, and Defendants' presence and continuous contact in Pennsylvania. Accordingly, Defendants have purposely availed themselves of the privilege of conducting activities within the State of Pennsylvania.

24. Further, this Court has personal jurisdiction over Defendants because Defendants' tortious conduct against Plaintiff occurred in substantial part within this District and because Defendant committed the same wrongful acts to other individuals within this judicial District, such that Defendants' acts complained of herein occurred within this District, subjecting Defendant to jurisdiction here. *See Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 132 (3d Cir. 2022) ("the place of interception is the point at which the signals were routed to [the session replay provider's] servers"). Thus, Defendant knew or should have known that it was causing harm to those individuals while they were in Pennsylvania such that it was foreseeable to Defendant that its interceptions would harm Plaintiff and other similarly-situated individuals located in Pennsylvania.

25. This Court has subject matter jurisdiction pursuant to 42. Pa. Cons. Stat. § 931(a). Venue is proper in this Court pursuant to 42. Pa. Cons. Stat. § 931(c).

26. Plaintiff has standing to maintain this action because he has a substantial, direct, and immediate interest in the subject matter of this case. Plaintiff was aggrieved and injured by Defendants' interceptive use of session replay technology in violation of WESCA, which provides that "[a]ny person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 42 Pa. Cons. Stat. § 5725(a). Accordingly, Plaintiff has statutory standing to maintain this action. *See Beverly Healthcare- Murrysville v. Dep't of Pub. Welfare*, 828 A.2d 491, 493 (Pa. Commw.

Ct. 2003) ("The concept of standing concerns the question of who is entitled to make a legal challenge to the matter involved. Standing may be conferred by a statute or by an interest of a party deserving legal protection").

FACTS

27. Defendants own and operate the following website: www.autozone.com.

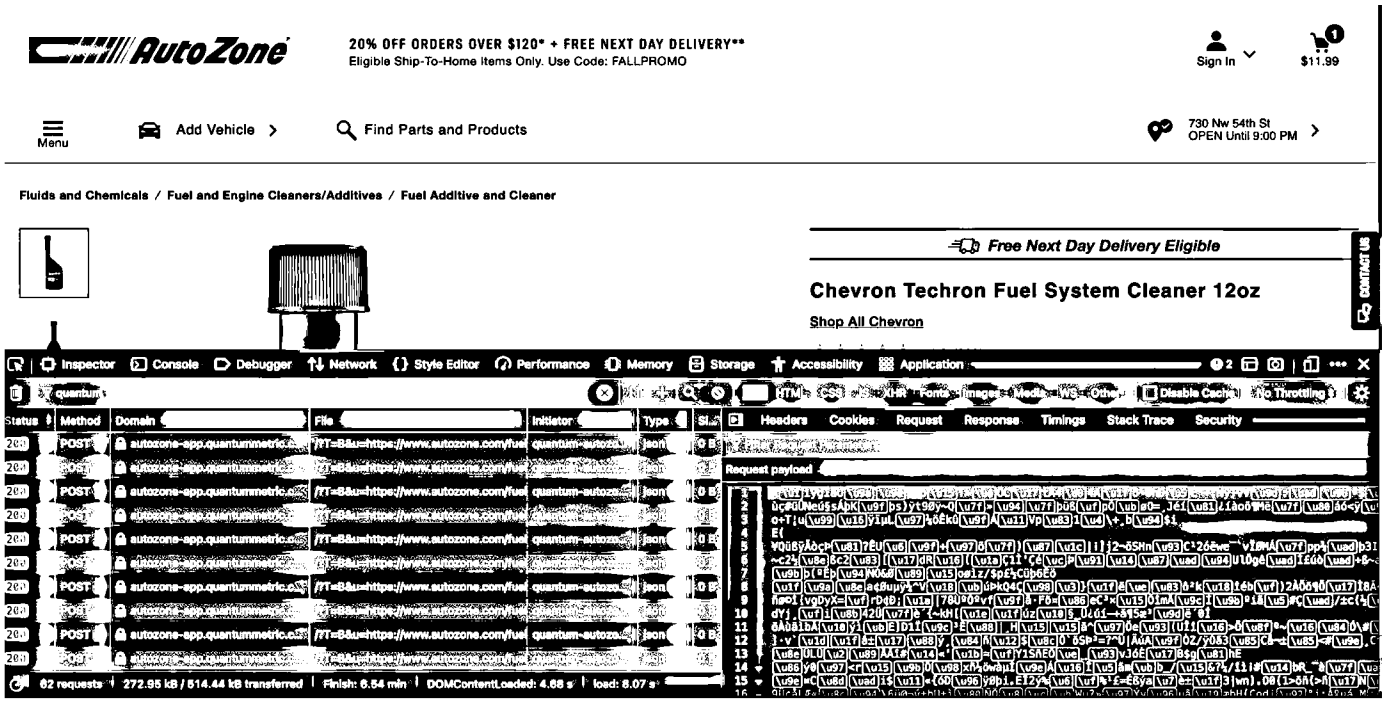
28. In 2022, Plaintiff visited Defendants' website approximately 10 or more times.

29. Plaintiff most recently visited Defendants' website on or about August 2022, to review car parts related to Plaintiff's auto business.

30. Plaintiff was in Pennsylvania during each visit to Defendants' website.

31. During his visits to the website, Plaintiff, through his computer and/or mobile device transmitted substantive information via electronic communications in the form of instructions to Defendants' computer servers utilized to operate the website.[6] The commands were sent as messages instructing Defendants what content was being viewed, clicked on, requested and/or inputted by Plaintiff. The following is an example of such a communication:

[6] These communications occur through the Hypertext Transfer Protocol ("HTTP"). HTTP works as a request-response protocol between a user and a server as the user navigates a website. A GET request is used to request data from a specified source. A POST request is used to send data to a server. *See HTTP Request Methods,* located at https://www.w3schools.com/tags/ref_httpmethods.asp (last visited November 16, 2022).



32. The communications sent by Plaintiff to Defendants' (and unknowingly to the Session Replay Providers') servers included, but were not limited to, the following actions taken by Plaintiff while on the website: mouse clicks and movements, keystrokes, search terms, information and PII inputted and communicated by Plaintiff, pages and content viewed by Plaintiff, scroll movements, and copy and paste actions. For every action on the website, the accorded HTTP message recorded not only what was done, where on the site, and what information was requested, but further included details about Plaintiff such as his location, his device, the URL, a unique session identifier, his internet service provider, and IP address. Indeed, each interaction caused a communication that contained substantive information about who Plaintiff was and what he was doing on the website.

33. Defendants responded to Plaintiff's electronic communications by processing and supplying – through the website – the information inputted and requested by Plaintiff. *See Revitch v. New Moosejaw, LLC*, No. 18-cv-06827-VC, 2019 U.S. Dist. LEXIS 186955, at *3 (N.D. Cal.

Oct. 23, 2019) ("This series of requests and responses — whether online or over the phone — is communication.").

34. Unbeknownst to Plaintiff, Defendants' transmitted and implanted session replay code directly onto Plaintiff's device which enabled the session replay software to intercept these communications.

35. At virtually the same moment that Plaintiff sent communications to Defendants' servers, the session replay software procured by Defendants instantaneously created a duplicate request-and-response transmission of each of Plaintiff's communications and routed these communications to the Session Replay Provider's servers

36. Plaintiff reasonably expected that his visits to Defendants' website would be private and that Defendants would not have procured a third party that would be tracking, recording, and/or watching Plaintiff as he browsed and interacted with the website, particularly because Plaintiff was never presented with any type of pop-up disclosure or consent form alerting Plaintiff that his visits to the website were being recorded by Defendants.

37. Plaintiff reasonably believed that he was interacting privately with Defendants' website, and not that he was being recorded and that those recordings would be captured and transmitted by and to third party servers that Plaintiff was unaware of, where they would be processed by that third party and could later be watched by Defendants' employees, or worse yet, live while Plaintiff was on the website.

38. Upon information and belief, over at least the past two years, Defendants have had embedded within the website code and has continuously operated at least one session replay script[7] that was provided by a third party (a "Session Replay Provider"). The session replay spyware was

[7] A script is a sequence of computer software instructions.

always active and, after being implanted on the visitor's device, intercepted every incoming data communication to Defendants' website the moment a visitor accessed the site.

39. The Session Replay Provider(s) that provided the session replay spyware to Defendants are not a provider of wire or electronic communication services, or an internet service provider.

40. Defendants are not a provider of wire or electronic communication services, or an internet service provider.

41. Defendants' use of session replay spyware was not instrumental or necessary to the operation or function of Defendants' website or business.

42. Defendants' use of a session replay spyware through a third party Session Replay Provider to intercept Plaintiff's electronic communications was not instrumental or necessary to Defendants' provision of any of its goods or services. Rather, the level and detail of information surreptitiously collected by Defendants' Session Replay Provider(s) indicates that the only purpose was to gain an unlawful understanding of the habits and preferences of users to its website, and the information collected was solely for Defendants' own benefit.

43. Defendants' use of a session replay spyware procured from a third party to intercept Plaintiff's electronic communications did not facilitate, was not instrumental, and was not incidental to the transmission of Plaintiff's or the Class members' electronic communications with Defendants' Website.

44. Upon information and belief, during one or more of Plaintiff's visits to Defendants' website, Defendants utilized session replay spyware procured from undisclosed third parties to intentionally and contemporaneously intercept the substance of Plaintiff's electronic communications with Defendants' website, including but not limited to mouse clicks and

movements, keystrokes, search terms, information inputted by Plaintiff, pages and content viewed by Plaintiff, scroll movements, copy and paste actions, descriptive URLS, device information, browser information, geolocation, Plaintiff's internet service provider, Plaintiff's unique session identifier. In other words, Defendant utilized its Session Replay Provider(s) to intercept, record, process and store electronic communications conveying, in detail, everything Plaintiff did on the webpages visited by Plaintiff i.e. what Plaintiff searched for, what Plaintiff looked at, and the detailed personal information that Plaintiff inputted.

45. The session replay spyware intentionally utilized by Defendants contemporaneously intercepted the electronic computer-to-computer data communications between Plaintiff's computer and/or mobile device and the computer servers and hardware utilized by Defendant to operate its website – as the communications were transmitted from Plaintiff's computer and/or mobile device to Defendants' computer servers and hardware – and copied and sent and/or re-routed the communications to a storage file within the Session Replay Provider(s)'s server(s). The intercepted data was transmitted contemporaneously to the Session Replay Provider(s) server(s) as it was sent from Plaintiff's computer and/or mobile device.

46. The relevant facts regarding the full parameters of the communications intercepted and how the interception occurred are solely within the possession and control of Defendants.

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

48. Unlike the harmless collection of an internet protocol address, the data collected by Defendants identified specific information inputted and content viewed (such as pages viewed, URLs, items clicked, information type, as well as Plaintiff's identifying information), and thus revealed personalized and sensitive information about Plaintiff's internet activity and habits.

49. The electronic communications intentionally intercepted at Defendants' behest were content generated through Plaintiff's intended use, interaction, and communication with Defendants' website relating to the substance, purport, and/or meaning of Plaintiff's communications with the website, *i.e.*, mouse clicks and movements, keystrokes, search terms, information inputted by Plaintiff, and pages and content clicked on and viewed by Plaintiff. As stated above, these communications were not a simple record of a mouse click occurring, but instead a mouse click specifically associated with Plaintiff through his various identifiers, as well as what he clicked on, where, when, etc.

50. The electronic communications intentionally intercepted by Defendants were not generated automatically and were not incidental to Plaintiff's communications.

51. The session replay spyware procured and utilized by Defendants intercepted, copied, replicated, and sent the data to the Session Replay Provider(s) in a manner that was undetectable by Plaintiff.

52. Plaintiff's electronic data communications were then, processed, interpreted, stored and reproduced by Defendants and/or the Session Replay Provider(s).

53. The electronic data communications were not only intercepted and stored, could also be used by Defendants to create a video playback of Plaintiff's visit to the website, displaying the content communicated by Plaintiff during his interactions with the site. Additionally, upon information and belief, the session replay technology procured by Defendants gave Defendants the ability to view Plaintiff's website visits live in real-time as they were occurring.

54. Defendants' procured interception of Plaintiff's electronic communications allowed Defendants to capture, observe, and divulge Plaintiff's personal details, interests, browsing history, queries, and habits as he interacted with and browsed Defendants' website.

55. Upon information and belief, Defendants similarly procured the interception of the electronic communications of more than 200,000 individuals located in Pennsylvania who visited Defendants' website.

56. Defendants utilized third party spyware embedded within the website and the services of its Session Replay Provider(s) to intercept the communications at issue.

57. Defendants never alerted or asked Plaintiff or the Class Members for permission to have its Session Replay Provider(s) intercept and record their visits to Defendants' Websites using "session replay" spyware.

58. Plaintiff and the Class members never consented to interception of their electronic communications by Defendants and/or it's Session Replay Provider(s) or anyone acting on Defendants' behalf, and they were never given the option to opt out of Defendants' recording.

59. At no point in time did Plaintiff or the Class members provide Defendants, their employees, or agents with consent to intercept their electronic communications using "session replay" spyware.

60. At no point in time did Plaintiff or the Class members specifically, clearly, and unmistakably consent to Defendants' use of a third party to intercept and record their electronic communications using "session replay" spyware.

61. At no point in time did Plaintiff or the Class members specifically, clearly, and unmistakably consent to Defendants' use of a third party to intercept and record of their visits to Defendants' Websites using "session replay" spyware.

62. At no point in time did Plaintiff or the Class members impliedly consent to Defendants' use of a third party to intercept and record their electronic communications, as no reasonable person could assume that by communicating with Defendants' website, the substance

of those electronic communications would be intercepted, captured, read, observed, re-routed, forwarded, interpreted, reproduced, and stored by an undisclosed third party Session Replay Provider.

63. Plaintiff and the Class members did not have a reasonable opportunity to discover Defendants' unlawful interceptions because Defendants did not disclose the third party interception nor seek consent from Plaintiff and the Class members prior to interception of their communications.

64. Plaintiff and the Class members never clicked or otherwise agreed to any disclosure or consent form authorizing Defendants to use a third party Session Replay Provider to intercept Plaintiff's and the Class members' electronic communications using "session replay" spyware.

65. Defendants' third party session replay spyware intercepted Plaintiff's and the Class members' electronic communications from the moment they landed on Defendants' Websites, and before they had an opportunity to even consider consenting or agreeing to any privacy or terms of use policy on the Websites. In other words, Defendants' unlawful interception occurred before Plaintiff and the Class members were given an opportunity to review, let alone provide prior consent, to any language that Defendants may claim purportedly authorized its violations of the WESCA. *See Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 U.S. App. LEXIS 14951, at *5 (9th Cir. May 31, 2022).

66. Moreover, Defendants' website failed to explicitly alert or otherwise notify Plaintiff and the Class members that Defendants would be utilizing session replay spyware to facilitate an undisclosed third party's monitoring and recording of their interactions with Defendants' Website.

67. Additionally, upon immediately landing on Defendants' Website, Plaintiff and the Class members were not alerted that by entering the website Defendants would unilaterally attempt to bind them to Defendants' terms of use or privacy policy. Indeed, the landing page to Defendants' website not only fails to advise visitors that Defendant is using a third party to intercept their electronic communications; it does not contain any type of conspicuous disclosure regarding Defendants' terms of use or privacy policy.

68. Plaintiff and the Class members were not immediately required to click on any box or hyperlink containing Defendants' terms of use or privacy policy upon visiting the Website or in order to navigate through the Website.

69. Plaintiff and the Class members were not placed on notice of Defendants' terms and policies or privacy policy upon immediately visiting the Website. Instead, Defendants' terms of use and privacy policy are buried at the bottom of Defendants' Website where Plaintiff and the Class members were unable to see them. These inconspicuous footer hyperlinks are insufficient to have put Plaintiff and the Class members on inquiry notice of Defendants' terms of use and privacy policy. *See Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1177 (9th Cir. 2014).

70. Defendants do not require visitors to its website to immediately and directly acknowledge that the visitor has read Defendants' terms of use or privacy policy before proceeding to the site. In other words, Defendants' website does not immediately direct visitors to the site to the terms of use or privacy policy, and does not require visitors to click on a box to acknowledge that they have reviewed the terms and conditions/policy in order to proceed to the website.

71. Upon information and belief, at least one of the purposes of Defendants' procured interception of Plaintiff's and the Class members' electronic communications was to allow Defendants to learn of Plaintiff's and the Class members' personal details, preferences and likes,

which would then be used to market Defendants' services and goods to Plaintiff and the Class members. Additionally, Defendants' violations of WESCA allowed undisclosed third parties to "fingerprint" Plaintiff and the Class members for their own uses through their substantive communications that were intended solely for Defendants.

72. The surreptitious third party interception of Plaintiff's and the Class members' electronic communications procured by Defendants caused Plaintiff and the Class members harm, including violations of their substantive legal privacy rights under the WESCA, invasion of privacy, intrusion upon seclusion, invasion of their rights to control information concerning their person, and/or the exposure of their private information. Indeed, at common law, the intrusion into Plaintiff's and the Class members' private lives is of itself a cognizable injury. Moreover, Defendants' practices caused harm, and a material risk of harm, to Plaintiff's and the Class Members' privacy and interest in controlling their personal information, habits, and preferences.

CLASS ALLEGATIONS

PROPOSED CLASS

73. Plaintiff brings this lawsuit as a class action on behalf of all other similarly situated persons pursuant to 231 Pa. Code Chapter 1700. The "Class" that Plaintiff seeks to represent is defined as:

> **All persons residing within the State of Pennsylvania (1) who visited Defendants' website and (2) whose electronic communications were intercepted by Defendant or on**

Defendants' behalf through session replay (3) without their prior consent.

74. Defendants and their employees or agents are excluded from the Class. Plaintiff reserves the right to modify or amend the Class definitions, as appropriate, during the course of this litigation.

NUMEROSITY (231 PA. CODE CHAPTER 1702(1))

75. The Class members are so numerous that individual joinder of all Class members is impracticable. Upon information and belief, Defendants intercepted the electronic communications of over 200,000 individuals. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include notice on Defendants' website, U.S. Mail, electronic mail, Internet postings, and/or published notice.

76. The identities of the Class members are unknown at this time and can be ascertained only through discovery. Identification of the Class members is a matter capable of ministerial determination from Defendants' records kept in connection with its unlawful interceptions.

77.

COMMON QUESTIONS OF LAW AND FACT (231 PA. CODE CHAPTER 1702(2)

78. There are numerous questions of law and fact common to the Class which predominate over any questions affecting only individual members of the Class. Among the questions of law and fact common to the Class are:

(1) Whether Defendants violated the WESCA;

(2) Whether Defendants intercepted or procured another to intercept Plaintiff's and the Class members' electronic communications;

(3) Whether Defendants disclosed to Plaintiff and the Class Members that they

were intercepting their electronic communications;

(4) Whether Defendants secured prior consent before intercepting Plaintiff's and the Class members' electronic communications; and

(5) Whether Defendants are liable for damages, and the amount of such damages.

79. The common questions in this case are capable of having common answers. If Plaintiff's claim that Defendants routinely intercepts electronic communications without securing prior consent is accurate, Plaintiff and the Class members will have identical claims capable of being efficiently adjudicated and administered in this case.

TYPICALITY (231 PA. CODE CHAPTER 1702(3))

80. Plaintiff's claims are typical of the claims of the Class members, as they are all based on the same factual and legal theories.

ADEQUACY (231 PA. CODE CHAPTER 1702(4))

81. Plaintiff is a representative who will fully and adequately assert and protect the interests of the Class and has retained competent counsel. Accordingly, Plaintiff is an adequate representative and will fairly and adequately protect the interests of the Class.

SUPERIORITY (231 PA. CODE CHAPTER 1702(5))

82. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the claims of all members of the Class is economically unfeasible and procedurally impracticable. While the aggregate damages sustained

by the Class are potentially in the millions of dollars, the individual damages incurred by each member of the Class resulting from Defendants' wrongful conduct are too small to warrant the expense of individual lawsuits. The likelihood of individual Class members prosecuting their own separate claims is remote, and, even if every member of the Class could afford individual litigation, the court system would be unduly burdened by individual litigation of such cases.

83. The prosecution of separate actions by members of the Class would create a risk of establishing inconsistent rulings and/or incompatible standards of conduct for Defendant. For example, one court might enjoin Defendants from performing the challenged acts, whereas another may not. Additionally, individual actions may be dispositive of the interests of the Class, although certain class members are not parties to such actions.

COUNT I
Violations of the WESCA, 18 Pa. Cons. Stat. 5701, *et seq.*
(On Behalf of Plaintiff and the Class)

84. Plaintiff re-alleges and incorporates the foregoing allegations as if fully set forth herein.

85. The Pennsylvania Wiretap and Electronic Surveillance Control Act (the "Act") prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was

obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

86. An "intercept[ion]" is the "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device". *See* 18 Pa. Cons. Stat. § 5702.

87. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

88. Defendants procured at least one third party Session Replay software to automatically and secretly spy on, and intercept, Defendants' website visitor's electronic communications with Defendants in real-time.

89. To facilitate this wiretap, Defendants procured and installed its Session Replay Provider's code on the website and implanted it on the Class members' devices.

90. In the context of wiretapping, software can constitute a device. *See United States v. Barrington*, 648 F.3d 1178, 1201 n.23 (11th Cir. 2011) (holding a device includes "innovative means that parties use to gain unauthorized information.")

91. The session replay software code procured from the Session Replay Provider(s) by Defendants is a sophisticated system capable of capturing, recording, interpreting, reformatting, and processing electronic communications, and is therefore an "electronic, mechanical, or other device" as defined by the WESCA. *See* 18 Pa. Cons. Stat. § 5702.

92. The session replayed software code procured from the Session Replay Provider(s) by Defendants is not a "tracking device" because, as stated above, it is a sophisticated system with capabilities well beyond "***only*** the tracking of the movement of a person or object." *See* 18 Pa. Cons. Stat. § 5702.

93. Upon information and belief, Defendants knew that their Session Replay Provider(s) would add the contents of their visitor's private electronic communications to its back-end database, resulting in the unauthorized disclosure of such information to the Session Replay Provider(s) and risking the further disclosure of that information to others.

94. Defendants intentionally procured the interception of the content of Defendants' website visitors' private electronic communications in real-time.

95. Plaintiff and the putative class members engaged in electronic communications with Defendants through use of Defendants' Website.

96. Plaintiff and the putative class members had a justified and reasonable expectation under the circumstances that their private electronic communications would not be intercepted by and exposed to an undisclosed third party. *See In re Google Inc.*, 806 F.3d 125, 151 (3d Cir. 2015); *see also In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 293-94 (3d Cir. 2016).

97. Nonetheless, Defendants employed its Session Replay Provider(s) to intercept the content of Plaintiff's and the putative class members' electronic communications with Defendant.

98. Because the code is secret and encrypted, Plaintiff and the putative class members were not aware that their electronic communications were being intercepted by Defendants' Session Replay Provider(s).

99. Plaintiff and the putative class members did not give prior consent to having their communications intercepted by Defendants or these Session Replay Provider(s).

100. By procuring Session Replay Provider(s) to intercept, record, interpret, reproduce and store Plaintiff's and the Class members private electronic communications for its own purposes without prior consent, Defendants violated 18 Pa. Cons. Stat. § 5703(1), (2) and (3).

101. At all times pertinent hereto, Defendants' conduct was knowing and intentional.

102. As a result of Defendants' conduct, and pursuant to § 5725 of the WESCA, Plaintiff and the other members of the putative Class were harmed and are each entitled to actual damages, liquidated damages, punitive damages, reasonable attorneys' fees and costs. 18 Pa. Cons. Stat § 5725(a).

WHEREFORE, Plaintiff, on behalf of himself and the other members of the Class, prays for the following relief:

a. An order certifying the Class and appointing Plaintiff as Class Representative and his counsel as Class Counsel;

b. An award of actual damages, statutory damages, liquidated damages, and/or punitive damages;

c. An aware of reasonable attorney's fees and costs; and

d. Such further and other relief the Court deems reasonable and just.

JURY DEMAND

Plaintiff and Class Members hereby demand a trial by jury on all issues so triable.

DOCUMENT PRESERVATION DEMAND

Plaintiff demands that Defendants take affirmative steps to preserve all records, lists, electronic databases or other itemizations associated with the allegations herein, including all records, lists, electronic databases or other itemizations in the possession of any vendors,

individuals, and/or companies contracted, hired, or directed by Defendants to assist in the alleged conduct.

Dated: June 7, 2024

Respectfully Submitted,

By: **MARCUS ZELMAN LLC**

/s/ Ari H. Marcus
Ari H. Marcus, Esq. (Pennsylvania Bar No. 322283)
Joseph H. Kanee, Esq. (*pro hac vice*}
701 Cookman Avenue, Suite 300
Asbury Park, New Jersey 07712
Telephone: (732) 695-3282
Fascimile: (732) 298-6256
Ari@marcuszelman.com
joseph@marcuszelman.com
Counsel for Plaintiff and Proposed Class