**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF MISSOURI**
**EASTERN DIVISION**

| | |
|---|---|
| ANN JONES, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>BLOOMINGDALES.COM, LLC,<br><br>Defendant. | Case No. 4:22-cv-1095<br><br>**JURY TRIAL DEMANDED** |

## COMPLAINT - CLASS ACTION

Plaintiff Ann Jones ("Plaintiff"), individually and on behalf of all others similarly situated, hereby files this class action complaint against Defendant Bloomingdales.com, LLC ("Defendant" or "Bloomingdale's"), and in support thereof alleges the following:

## INTRODUCTION

1. This is a class action brought against Bloomingdale's for surreptitiously intercepting and wiretapping the electronic communications of visitors to its website, www.bloomingdales.com. Bloomingdale's procures third-party vendors, such as FullStory, to embed snippets of JavaScript computer code ("Session Replay Code") on Bloomingdale's website, which then deploys on each website visitor's internet browser for the purpose intercepting and recording the website visitor's electronic communications with the Bloomingdale's website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications

in real-time ("Website Communications"). These third-party vendors (collectively, "Session Replay Providers") create and deploy the Session Replay Code at Bloomingdale's request.

2. After intercepting and capturing the Website Communications, Bloomingdale's and the Session Replay Providers use those Website Communications to recreate website visitors' entire visit to www.bloomingdales.com. The Session Replay Providers create a video replay of the user's behavior on the website and provide it to Bloomingdale's for analysis. Bloomingdale's directive to the Session Replay Providers to secretly deploy the Session Replay Code results in the electronic equivalent of "looking over the shoulder" of each visitor to the Bloomingdale's website for the entire duration of their website interaction.

3. Bloomingdale's conduct violates the Missouri Wiretap Act, Mo. Ann. Stat. §§ 542.400 *et seq.*, the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010 *et seq*., and constitutes an invasion of the privacy rights of website visitors.

4. Plaintiff brings this action individually and on behalf of a class of all Missouri citizens whose Website Communications were intercepted through Bloomingdale's procurement and use of Session Replay Code embedded on the webpages of www.bloomingdales.com and seeks all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, and attorneys' fees and costs.

## PARTIES

5. Plaintiff Ann Jones is a citizen of the State of Missouri, and at all times relevant to this action, resided and was domiciled in St. Louis County, Missouri. Plaintiff is a citizen of Missouri.

6. Defendant Bloomingdales.com, LLC is a corporation organized under the laws of Ohio, and its principal place of business is located at 3 Jackson Tower, 20th Floor, 28-07 Jackson

Avenue, Long Island City, NY 11101. Defendant is deemed a citizen of Ohio and New York. Defendant can be served through its registered agent Corporate Creations Network Inc. located at 600 Mamaroneck Avenue, Suite 400, Harrison, NY, 10528.

## JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class, including Plaintiff, is a citizen of a state different than Defendant.

8. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in Missouri. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of Missouri while they were located within Missouri. At all relevant times, Defendant knew that its practices would directly result in collection of information from Missouri citizens while those citizens browse www.bloomingdales.com. Defendant chose to avail itself of the business opportunities of marketing and selling its goods in Missouri and collecting real-time data from website visit sessions initiated by Missourians while located in Missouri, and the claims alleged herein arise from those activities.

9. Bloomingdale's also knows that many users visit and interact with Bloomingdale's websites while they are physically present in Missouri. Both desktop and mobile versions of Bloomingdale's website allow a user to search for nearby stores by providing the user's location, as does the Bloomingdale's app. Users' employment of location services in this way means that Bloomingdale's is continuously made aware that its website is being visited by people located in

Missouri, and that such website visitors are being wiretapped in violation Missouri statutory and common law.

10. 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.

## FACTUAL ALLEGATIONS

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

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

12. Earlier this year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business's website, applications, and emails), behavioral data (*i.e.*, customers' purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.[2] This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.[3]

13. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success.

---

[1] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data.

[2] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, Business News Daily (Aug. 5, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

[3] *Id.*

Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[4]

14. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[5] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[6]

15. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[7]

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

16. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that "a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected."[8]

---

[4] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.

[5] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

[6] *Id.* at 25.

[7] *Id.*

[8] Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/.

17. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.[9] As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[10]

18. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

19. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[11]

20. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[12]

21. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing

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

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

[11] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

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

companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[13]

**C. How Session Replay Code Works.**

22. Session Replay Code, such as that implemented on www.bloomingdales.com, enables website operators to record, save, and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with insights into the user experience by recording website visitors "as they click, scroll, type or navigate across different web pages."[14]

23. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website operator, or has not finished submitting the data to the website operator.[15] As a result, website visitors "aren't just sharing data with the [web]site they're on . . . but also with an analytics service that may be watching over their shoulder."[16]

---

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

[14] Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/.

[15] *Id.*

[16] Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0.

24. Session Replay Code works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the occurrence of actions the user takes. When a website delivers Session Replay Code to a user's browser, the browser will follow the code's instructions by sending responses in the form of "event" data to a designated third-party server. Typically, the server receiving the event data is controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

25. The types of events captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user's navigation and interaction through the website. In order to permit a reconstruction of a user's visit accurately, the Session Replay Code must be capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are typically accumulated and transmitted in blocks periodically throughout the user's website session, rather than after the user's visit to the website is completely finished.

26. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the Session Replay Provider.

27. Once the events from a user session have been recorded by a Session Replay Code, a website operator can view a visual reenactment of the user's visit through the Session Replay Provider, usually in the form of a video, meaning "[u]nlike typical analytics services that provide

aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions."[17]

28. Because most Session Replay Codes will by default indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.[18]

29. Most alarming, Session Replay Code may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a "submit" or "enter" button on the website, the Session Replay Code may nevertheless cause the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the Session Replay Provider.

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

31. First, if a user's entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

[17] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.
[18] *Id.*

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

33. Third, some Session Replay Providers explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.[19]

34. Session Replay Providers often create "fingerprints" that are unique to a particular user's combination of device and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the Session Replay Provider monitors.

35. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user's other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

36. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.[20] Indeed, "[t]he more copies of sensitive information that exist, the broader the attack surface, and when data is being collected [

[19] *Id.*; *see also FS.identify – Identifying users*, FullStory, https://help.fullstory.com/hc/en-us/articles/360020828113, (last visited Sep. 8, 2022).
[20] Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720.

] it may not be stored properly or have standard protections" increasing "the overall risk that data will someday publicly leak or be breached."[21]

37. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from the app store.[22] In announcing this decision, Apple stated: "Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity."[23]

### D. Bloomingdale's Secretly Wiretaps its Website Visitors' Electronic Communications.

38. Bloomingdale's operates the website www.bloomingdales.com. Bloomingdale's is an online and brick-and-mortar fashion retailer, offering men's and women's apparel, accessories, shoes, and more.

39. However, unbeknownst to the millions of individuals perusing Bloomingdale's products online, Bloomingdale's intentionally procures and embeds various Session Replay Codes from Session Replay Providers on its website to track and analyze website user interactions with www.bloomingdales.com. Because the Session Replay Providers are unknown eavesdroppers to visitors to www.bloomingdales.com, they are not parties to website visitors' Website Communications with Bloomingdale's.

---

[21] Lily Hay Newman, *Covert 'Replay Sessions' Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/.

[22] Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), https://techcrunch.com/2019/02/07/apple-glassbox-apps/.

[23] *Id.*

40. One such Session Replay Provider that Bloomingdale's engages is FullStory.

41. FullStory is the owner and operator of a Session Replay Code titled FullStory Script, which records all website visitor actions, including information typed by the website users while on the website. Such information can include names, emails, phone numbers, addresses, social security numbers, date of birth, and more; research by the Princeton University Center for Information Technology Policy found that "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."[24]

42. As a user interacts with any website with the embedded FullStory Script, "each click, tap, URL visit, and every other interaction is sent in tiny little packets to that existing session at FullStory servers."[25] This includes button clicks, mouse movements, scrolling, resizing, touches (for mobile browsers), key presses, page navigation, changes to visual elements in the browsers, network requests, and more.[26]

43. Bloomingdale's knowingly derives a benefit and/or information from the Website Communications intercepted and recorded at its direction. Upon information and belief, Bloomingdale's uses the intercepted Website Communications to replay website visitors' interactions with www..bloomingdales.com, improve user interactions with its website, and to provide targeted advertisements to its website visitors.

---

[24] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

[25] *Id.*

[26] *How does FullStory capture data to recreate my users' experience?*, FullStory, https://help.fullstory.com/hc/en-us/articles/360032975773-How-does-FullStory-capture-data-to-recreate-my-users-experience-, (last visited Aug. 18, 2022) (hereinafter "FullStory Data Capture").

44. Bloomingdale's procurement and use of FullStory's Session Replay Code, and procurement and use of other Session Replay Codes through various Session Replay Providers, and its knowing derivation of a benefit and/or information from the Website Communications surreptitiously intercepted and recorded by Session Replay Codes is a violation of Missouri statutory and common law.

**E. Plaintiff's and Class Members' Experience.**

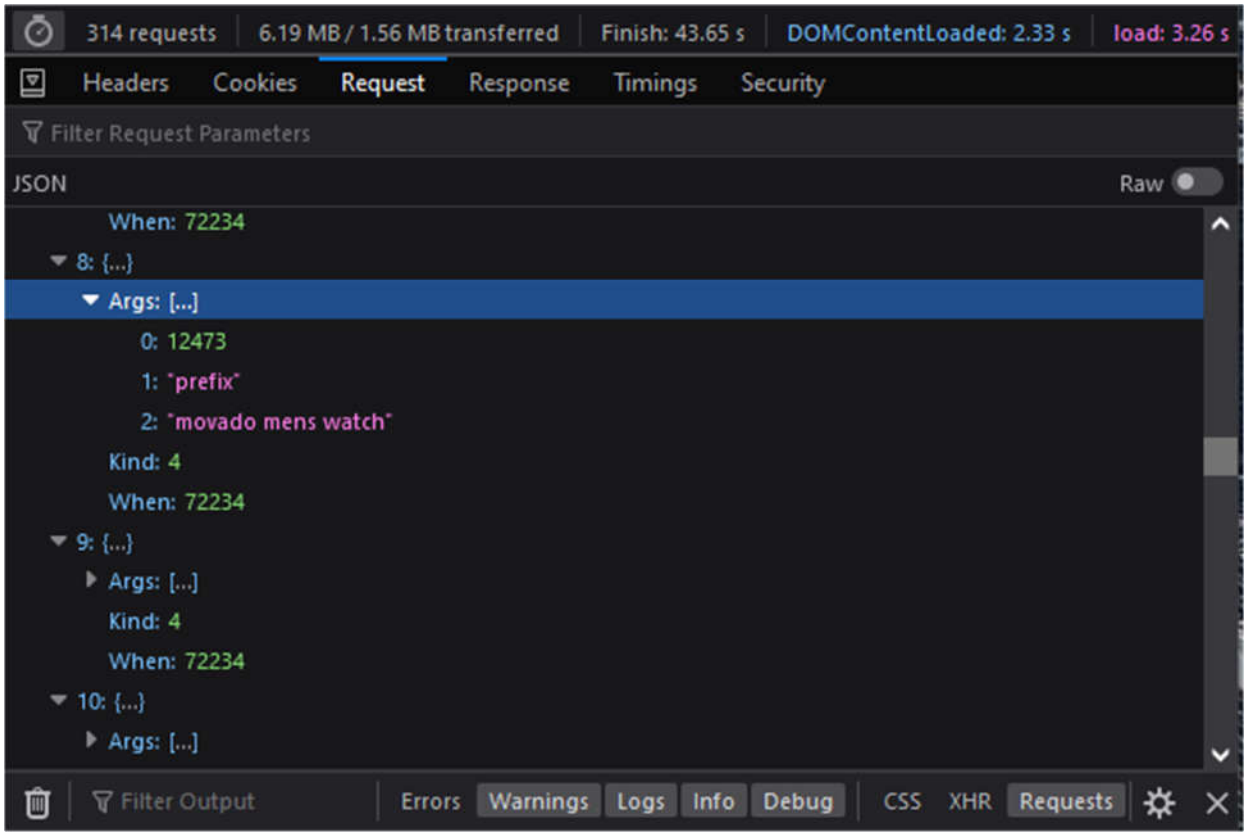
45. Plaintiff has visited www.bloomingdales.com while in Missouri. Specifically, Plaintiff visited www.bloomingdales.com via the web browser on both her mobile phone and computer.

46. While visiting Bloomingdale's website, Plaintiff fell victim to Defendant's unlawful monitoring, recording, and collection of Plaintiff's Website Communications with www.bloomingdales.com.

47. Unknown to Plaintiff, Bloomingdale's procures and embeds Session Replay Code on its website.

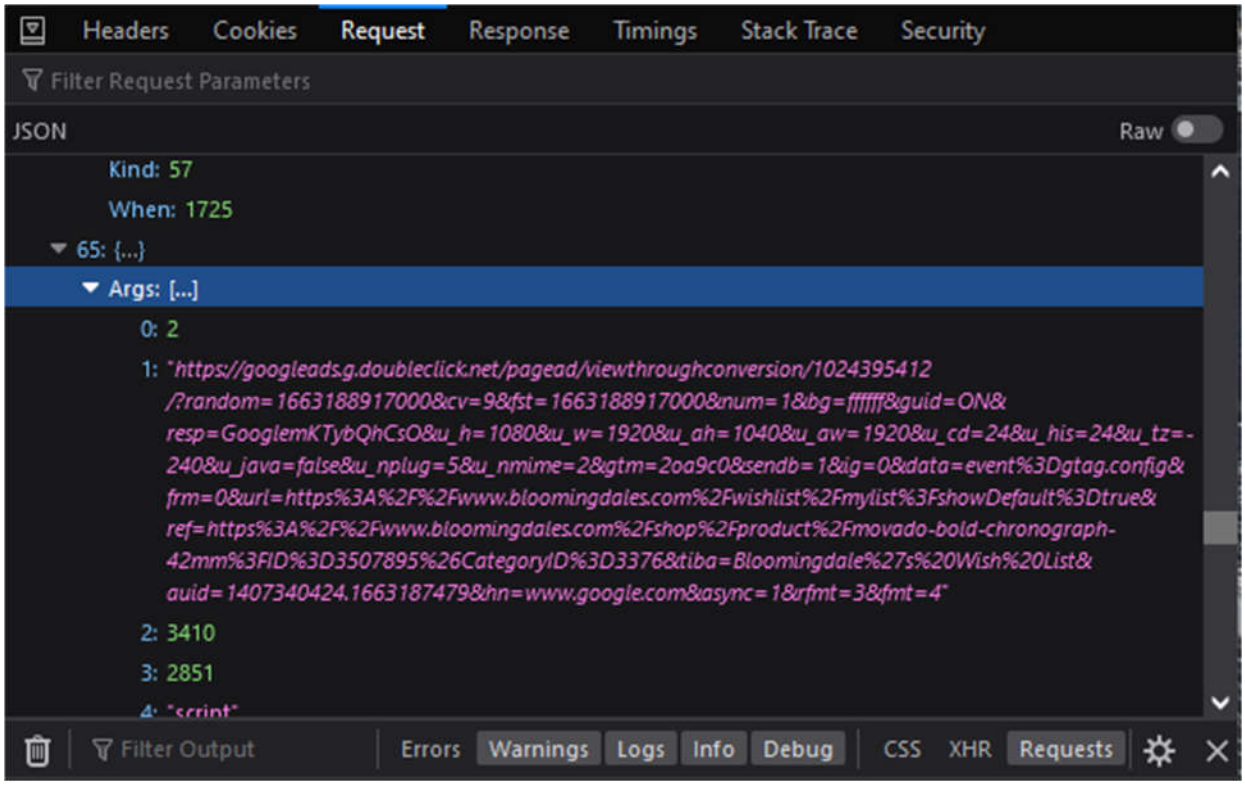
48. During the website visit, Plaintiff's Website Communications were captured by Session Replay Code and sent to various Session Replay Providers.

49. For example, when visiting www.bloomingdales.com, if a website user views a product, that information is captured by the Session Replay Codes embedded on the website:



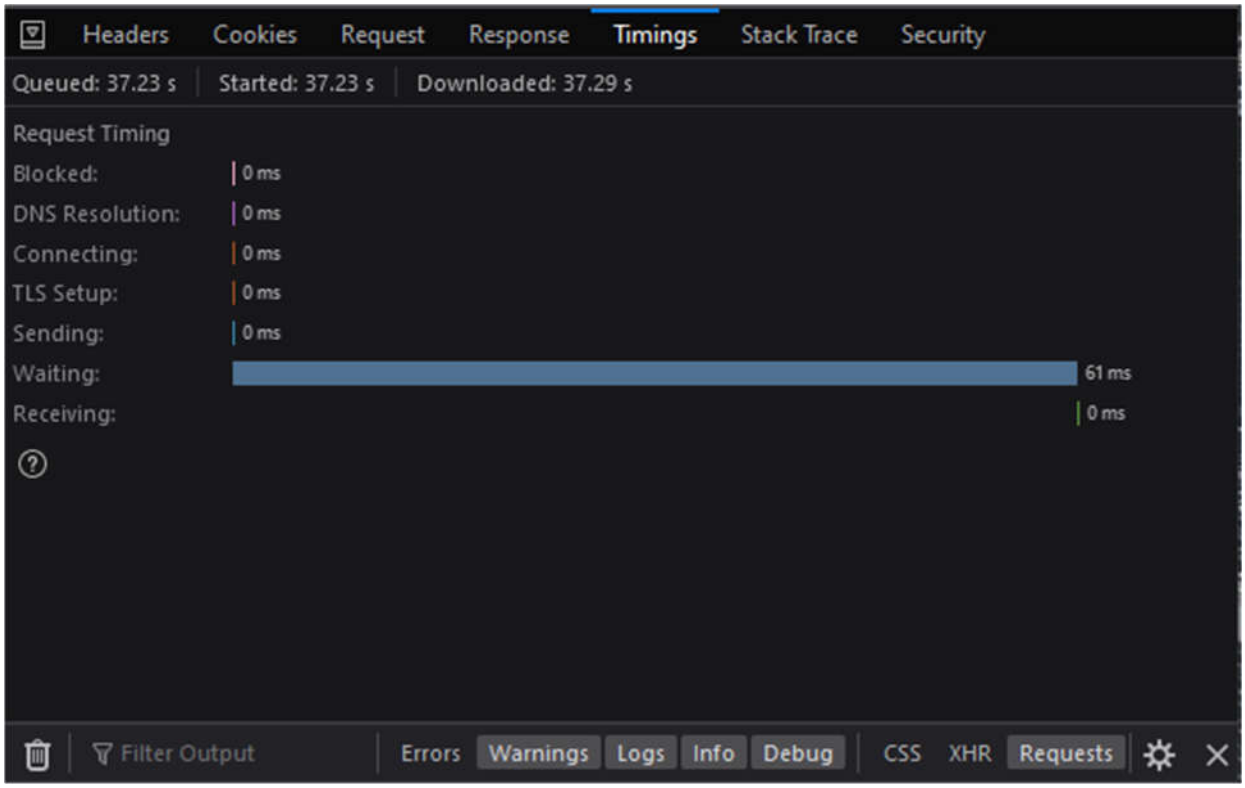

*Depicting information sent to one of the Service Replay Providers—FullStory—through a Service Replay Code—FullStory Script—after searching for "movado mens watch" while visiting* www.bloomingdales.com.

50. Similarly, when a user adds a product onto their "Wish List" on www.bloomingdales.com, that information is sent to Service Replay Providers:




*Depicting information sent to one of the Service Replay Providers—FullStory—through a Service Replay Code—FullStory Script—after adding a "Movado BOLD Chronograph, 42 mm" to a wish list on [www.bloomingdales.com](http://www.bloomingdales.com).*

51. The eavesdropping by the Session Replay Codes is ongoing during the visit and intercepts the contents of these communications between Plaintiff and Bloomingdale's with instantaneous transmissions to the Session Replay Provider(s), as illustrated below, in which only 61 milliseconds were required to send a packet of even response data, which would indicate whatever the website user had just done:




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

53. Like Plaintiff, each Class member visited www.bloomingdales.com with Session Replay Code embedded in it, and those Session Replay Codes intercepted the Class members' Website Communications with www.bloomingdales.com by sending hyper-frequent logs of those communications to Session Replay Providers.

54. Even if Bloomingdale's masks certain elements when it configures the settings of the Session Replay Code embedded on its website, any operational iteration of the Session Replay Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

55. For example, even with heightened masking enabled, Session Replay Providers will still learn through the intercepted data exactly which pages a user navigates to, how the user moves

through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

56. As a specific example, if a user types a product into Bloomingdale's main search bar and initiates a search, even if the text entered into the search bar is masked, Session Replay Providers will still learn what is entered into the bar as soon as the search result page loads. This is so because the responsive search results will be displayed on the subsequent page, and the responsive content generated by Bloomingdale's will repeat the searched information back on the generated page. That information will not be masked even if user-inputted text is fully masked in a text field.

## CLASS ACTION ALLEGATIONS

57. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

> All natural persons in the State of Missouri whose Website Communications were captured through the use of Session Replay Code embedded in www.bloomingdales.com.

58. Excluded from the Class are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the Class, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

59. **Numerosity:** The members of the Class are so numerous that individual joinder of all Class members is impracticable. The precise number of Class members and their identities may be obtained from the books and records of Bloomingdale's or the Session Replay Providers.

60. **Commonality:** This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to: (a) whether Defendant

employed Session Replay Providers to intercept and record Bloomingdale's website visitors' Website Communications; (b) whether Defendant operated or participated in the operation of an eavesdropping device; (c) whether Defendant derives a benefit or information from the illegal use of an eavesdropping device; (d) whether Defendant directed another to use an eavesdropping device illegally on its behalf; (e) whether Session Replay Code is an "eavesdropping device" used to intercept or record private electronic communications; (f) whether Defendant acquired the contents of website users' private electronic communications without their consent; (g) whether Plaintiff and Class members had a reasonable expectation of privacy in their Website communications; (f) whether Defendant violated the Missouri Wiretap Act, Mo. Ann. Stat. §§ 542.400 *et seq*.; (g) whether Defendant's interception of Plaintiff's and Class members' private electronic communications is an unfair or deceptive act or practice; (h) whether Defendant's conduct violates the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010 *et seq.* (i) whether Plaintiff and Class members are entitled to equitable relief; and (j) whether Plaintiff and Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

61. **Typicality:** Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiff and each member of the Class had their electronic communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiff and the members of the Class typical of one another.

62. **Adequacy of Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent

and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor her counsel have any interest adverse to the interests of the other members of the Class.

63. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

64. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant intercepted Plaintiff's and Class members' Website Communications, then Plaintiff and each Class member suffered damages by that conduct.

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

**COUNT I**
**Violation of Missouri Wiretap Act,**
**Mo. Ann. Stat. §§ 542.400 *et seq.***

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

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

68. The Missouri wiretap statute broadly prohibits the interception, disclosure or use of any wire, oral or electronic communication. Mo. Stat. § 542.402.

69. Any person whose wire communication is intercepted, disclosed, or used in violation of sections 542.400 to 542.422 shall (1) 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 communications; and (2) be entitled to recover from any such person: (a) actual damages, but not less than liquidated damages computed at the rate of one hundred dollars a day for each day of violation or ten thousand dollars whichever is greater; (b) punitive damages on a showing of a willful or intentional violation of sections 542.400 to 542.422; and (c) A reasonable attorney's fee and other litigation costs reasonably incurred. Mo. Stat. § 542.418.

70. "Wire communication" is defined as "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception including the use of such connection in a switching station furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of local, state or interstate communications." Mo. Stat. § 542.400(12).

71. A "Person" is "defined as any employee, or agent of this state or political subdivision of this state, and any individual, partnership, association, joint stock company, trust, or corporation." Mo. Stat. § 542.400(9).

72. "Intercept" is defined as "the aural acquisition of the contents of any wire communication through the use of any electronic or mechanical device, including but not limited to interception by one spouse of another spouse." Mo. Stat. § 542.400(6).

73. "Electronic, mechanical, or other device" is defined as "any device or apparatus which can be used to intercept a wire communication other than: (a) Any telephone or telegraph instrument, equipment or facility, or any component thereof, owned by the user or furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or being used by a communications common carrier in the ordinary course of its business or by an investigative office or law enforcement officer in the ordinary course of his duties; or (b) A hearing aid or similar device being used to correct subnormal hearing to not better than normal." Mo. Stat. § 542.400(5).

74. "Contents," "when used with respect to any wire communication, includes any information concerning the identity of the parties, the substance, purport, or meaning of that communication." Mo. Stat. § 542.400(3).

75. An "Aggrieved person" is defined as "a person who was a party to any intercepted wire communication or a person against whom the interception was directed." Mo. Stat. § 542.400 (1).

76. Bloomingdale's is a "Person" for purposes of the Act because it is a corporation.

77. Session Replay Code like that operated and employed at Bloomingdale's direction is an "electronic, mechanical or other device" used to transcribe electronic communications and to intercept a wire communication within the meaning of the Act.

78. The Session Replay Providers are not a party to the Website Communications—Plaintiff and the Class only knew they were communicating with Bloomingdale's, not the Session

Replay Providers.

79. Plaintiff's and Class members' intercepted Website Communications constitute wire communications within the meaning of the Act.

80. Bloomingdale's intentionally operated and employed Session Replay Code on its website to spy on, automatically and secretly, and intercept its website visitors' private electronic interactions communications with Bloomingdale's in real time, which are Contents within the meaning of the Act.

81. Plaintiff's and Class members' private electronic communications were intercepted contemporaneously with their transmission.

82. Plaintiff and Class members had a reasonable expectation of privacy in their Website Communications based on the detailed information the Session Replay Code collected from Plaintiff and Class members.

83. Plaintiff and Class members did not consent to having their Website Communications surreptitiously intercepted and recorded and are Aggrieved persons within the meaning of the Act.

84. Pursuant to Mo. Stat. § 542.418, Plaintiff and Class members are entitled to: (1) actual damages; (2) statutory damages including liquidated damages at $100 per day of violation or $10,000, whichever is greater, and (3) punitive damages. Plaintiff is also entitled to an award of attorney's fees and expenses.

85. Bloomingdale's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

**COUNT II**
**Violation of Missouri's Merchandising Practices Act**
**Mo. Rev. Stat. § 407.010 *et seq.***

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

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

88. The Missouri Merchandising Practice Act (for the purposes of this section, "MPA") protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

89. The Missouri MPA makes unlawful the "act, use or employment by any person of any deception, fraud, false pretense, misrepresentation, unfair practice, or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce." Mo. Rev. Stat. § 407.020.

90. Plaintiff, individually and on behalf of the Class, is entitled to bring this action pursuant to Mo. Rev. Stat. § 407.025, which provides in relevant part that: (a) Any person who purchases or leases merchandise primarily for personal, family or household purposes and thereby suffers an ascertainable loss of money or property, real or personal, as a result of the use or employment by another person of a method, act or practice declared unlawful by section 407.020, may bring a private civil action in either the circuit court of the county in which the seller or lessor resides or in which the transaction complained of took place, to recover actual damages. The court may, in its discretion, award to the prevailing party attorney's fees, based on the amount of time reasonably expended, and may provide such equitable relief as it deems necessary or proper.

91. Bloomingdale's is a "person" within the meaning of the Mo. Rev. Stat. § 407.010(5) in that Bloomingdale's is a domestic "[…] for-profit […] corporation."

92. Plaintiff and members of the Class are "persons" under the MMPA in that they are

natural persons, and they visited www.bloomingdales.com to utilize the Bloomingdale's search engine for personal, family, and/or household use. Furthermore, Plaintiff Ann Jones visited www.bloomingdales.com to utilize the Bloomingdale's search engine to shop for, purchase, and/or contract to purchase "merchandise" for personal, family, and/or household use.

93. The MPA applies to Bloomingdale's conduct described herein because it protects consumers in transactions that are intended to result, or which have resulted in the sale of goods or services.

94. The MMPA defines "merchandise" as any objects, wares, goods, commodities, intangibles, real estate, or services. *See* Mo. Rev. Stat. § 407.010. Thus, the items for sale on www.bloomingdales.com are merchandise within the meaning of the Act. Additionally, the website and the search engine thereon is a service which is used by Bloomingdale's in connection with the sale or advertisement of any merchandise in trade or commerce.

95. "Trade" or "commerce" is defined as "the advertising, offering for sale, sale, or distribution, or any combination thereof, of any services and any property, tangible or intangible, real, personal, or mixed, and any other article, commodity, or thing of value wherever situated." Bloomingdale's advertising, offering for sale, and sale of its real estate search engine and the real estate located thereon on www.bloomingdales.com is considered "trade" or "commerce" in the State of Missouri within the meaning of Mo. Rev. Stat. § 407.010(7).

96. The Missouri Attorney General has promulgated regulations defining the meaning of unfair practice as used in the above statute. Specifically, Mo. Code Regs. tit. 15, § 60-8.020, provides:

(1) An unfair practice is any practice which—

(A) Either—

1. Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or

2. Is unethical, oppressive or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers.

(2) Proof of deception, fraud, or misrepresentation is not required to prove unfair practices as used in section 407.020.1., RSMo. (*See, Federal Trade Commission v. Sperry and Hutchinson Co.*, 405 U.S. 233, 92 S.Ct. 898, 31 L.Ed.2d 170 (1972); *Marshall v. Miller*, 302 N.C. 539, 276 S.E.2d 397 (N.C. 1981); *see also*, Restatement, Second, Contracts, sections 364 and 365).

97. Pursuant to Mo. Rev. Stat. §407.020 and Mo. Code Regs. Tit. 15, § 60- 8.020, Defendant's acts and omissions fall within the meaning of "unfair."

98. Missouri case law provides that the MMPA's "literal words cover *every practice imaginable and every unfairness to whatever degree*." *Conway v. CitiMortgage, Inc.*, 438 S.W.3d 410, 416 (Mo. 2014) (quoting *Ports Petroleum Co., Inc. of Ohio v. Nixon*, 37 S.W.3d237, 240 (Mo. banc 2001). Furthermore, the statute's "plain and ordinary meaning of the words themselves . . . are unrestricted, all-encompassing and exceedingly broad." *Id.* at 240.

99. Bloomingdale's violated the MMPA by omitting and/or concealing material facts about www.bloomingdales.com. Specifically, Bloomingdale's omitted and/or concealed that it directed Session Replay Providers to secretly monitor, collect, transmit, and discloses its website visitors' Website Communications to the Session Replay Providers using Session Replay Code.

100. Bloomingdale's direction and employment of the Session Replay Providers and their Session Replay Codes to intercept, collect, and disclose website visitors' Website Communications are material to the transactions on www.bloomingdales.com. Bloomingdale's

does not disclose its use of Session Replay Code to secretly monitor and collect website visitors' Website Communications. Had Plaintiff and Class members known that the Session Replay Codes (that collect, transmit, and disclose Website Communications to the Session Replay Providers) were embedded in Bloomingdale's website, they would not have visited www.bloomingdales.com to shop for, purchase, or contract to purchase merchandise or they would have required Bloomingdale's to compensate them for the interception, collection, and disclosure of their Website Communications.

101. Bloomingdale's intentionally concealed the interception, collection, and disclosure of website visitors' Website Communications using Session Replay Code embedded in www.bloomingdales.com is material because it knows that consumers would not otherwise visit its website to search for, purchase, and contract to purchase merchandise. Indeed, Bloomingdale's concealment of such facts was intended to mislead consumers.

102. Bloomingdale's concealment, suppression, and/or omission of material facts was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the MMPA.

103. By failing to disclose and inform Plaintiff and the Class about its interception, collection, and disclosure of website visitors' Website Communications, Bloomingdale's engaged in acts and practices that constitute unlawful practices in violation of Mo. Ann. Stat. §§ 407.010, *et seq*.

104. As a direct and proximate result of these unfair and deceptive practices, Plaintiff and each member of the Class has suffered actual harm in the form of money and/or property because the disclosure of their Website Communications has value as demonstrated by the collection and use of it by Bloomingdale's. The collection and use of this information has now

diminished the value of such information to Plaintiff and the Class.

105. As such, Plaintiff and the Class seek an order (1) requiring Bloomingdale's to cease the unfair practices described herein; (2) awarding actual damages; and (3) awarding reasonable attorneys' fees and costs. Plaintiff and the Class seek all relief available under Mo. Ann. Stat. § 407.020, which prohibits "the act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce…," as further interpreted by Mo. Code Regs. Ann. tit. 15, §§ 60-7.010, *et seq.*, Mo. Code Regs. Ann. tit. 15, §§ 60-8.010, *et seq.*, and Mo. Code Regs. Ann. tit. 15, §§ 60-9.010, *et seq.*, and Mo. Ann. Stat. § 407.025, which provides for the relief sought in this count.

106. Bloomingdale's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

## COUNT III
### Invasion of Privacy – Intrusion Upon Seclusion

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

108. Under Missouri law, the general tort of invasion of privacy describes four distinct torts under Missouri law: (1) unreasonable intrusion upon the seclusion of another; or (2) appropriation of the other's name or likeness; or (3) unreasonable publicity given to the other's private life; or (4) publicity that unreasonably places the other in a false light before the public. Plaintiff brings this claim individually and on behalf of the Class. Plaintiff states a claim for unreasonable intrusion upon the seclusion of another.

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

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

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

112. Plaintiff and Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

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

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

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

116. Bloomingdale's conduct has needlessly harmed Plaintiff and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

117. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff and Class members of the economic value of their interactions with

Defendant's website, without providing proper consideration for Plaintiff's and Class members' property.

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

119. As a direct and proximate result of Bloomingdale's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

120. Bloomingdale's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

**TRESPASS TO CHATTELS**

121. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

122. Plaintiff owned, possessed, and/or had a right to possess Plaintiff's computer and/or the data in contained therein.

123. Plaintiff owned, possessed, and/or had a right to possess Plaintiff's mobile device and/or the data in contained therein.

124. As set forth above, Defendant intentionally interfered with: (a) Plaintiff's use and/or possession of Plaintiff's computer and mobile device; and/or (b) Plaintiff's use and/or possession of the data contained on Plaintiff's computer and/or mobile device as described above.

125. Plaintiff did not consent to the aforementioned interference.

126. The aforementioned interference was the actual and proximate cause of injury to Plaintiff and Class members because it exposed their private and/or personally identifiable information and/or data to one or more third parties.

127. Additionally, the interference gave third parties the data and information without the consent of Plaintiff and which is valuable and for which Defendant did not obtain informed consent nor pay Plaintiff to obtain.

128. Plaintiff and Class members are entitled to recover the actual damages they suffered as a result of Defendant's aforementioned interference with their computer and mobile devices in an amount to be determined at trial.

## REQUEST FOR RELIEF

Plaintiff, individually and on behalf of the other members of the proposed Class, respectfully request that the Court enter judgment in Plaintiff's and the Class's favor and against Defendant as follows:

A. Certifying the Class and appointing Plaintiff as the Class representative;

B. Appointing Plaintiff's counsel as class counsel;

C. Declaring that Defendant's past conduct was unlawful, as alleged herein;

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

E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;

F. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive,[27] and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

[27] Recent changes to the Missouri Merchandising Practices Act (MMPA) provide that:

G. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

**DEMAND FOR JURY TRIAL**

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

Date: October 14, 2022

*/s/ Tiffany Marko Yiatras*

Tiffany Marko Yiatras, MOED Bar No. 58197MO
CONSUMER PROTECTION LEGAL, LLC
308 Hutchinson Road
Ellisville, Missouri 63011-2029
Tele: 314-541-0317
Email: tiffany@consumerprotectionelegal.com

Bryan L. Bleichner (MN #0326689), to seek admission *pro hac vice*
**CHESTNUT CAMBRONNE PA**
100 Washington Avenue S, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300

---

> A claim for punitive damages shall not be contained in the initial pleading and may only be filed as a written motion with permission of the court no later than 120 days prior to the final pretrial conference or trial date. The written motion for punitive damages must be supported by evidence. The amount of punitive damages shall not be based on harm to nonparties. A pleading seeking a punitive damage award may be filed only after the court determines that the trier of fact could reasonably conclude that the standards for a punitive damage award, as provided in the act, have been met. The responsive pleading shall be limited to a response of the newly amended punitive damages claim.

Thus, Plaintiffs expressly disclaim punitive damages in this initial pleading; however, expect to file as a written motion with permission of the Court no later than 120 days prior to the final pretrial conference or trial date seeking punitive damages.

Fax: (612) 336-2940
bbleichner@chestnutcambronne.com

Kate M. Baxter-Kauf (MN #0392037), to seek admission *pro hac vice*
Karen Hanson Riebel (MN #0219770), to seek admission *pro hac vice*
Maureen Kane Berg (MN #033344X), to seek admission *pro hac vice*
**LOCKRIDGE GRINDAL NAUEN P.L.L.P.**
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com
mkberg@locklaw.com

*Attorneys for Plaintiff and the putative Class*