

**UNITED STATES DISTRICT COURT
DISTRICT OF COLORADO**

JALLEH DOTY and JEFFREY OGDEN,
individually and on behalf of all others similarly
situated,

Plaintiffs,

v.

QUANTUM METRIC, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Jalleh Doty and Jeffrey Ogden (“Plaintiffs”), individually and on behalf of all others similarly situated, by and through their attorneys, make the following allegations pursuant to the investigation of their counsel and based upon information and belief, except as to allegations specifically pertaining to themselves and their counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action suit brought against Defendant Quantum Metric, Inc. (“QM” or “Defendant”) for wiretapping the electronic communications of visitors to CVS’s website, cvs.com (the “Website”). The wiretaps, which are embedded in the computer code on the Website, are used by Defendant to secretly observe and record website visitors’ keystrokes, mouse clicks,¹ and other electronic communications, including Personally Identifiable Information (“PII”), such as users’ prescription and over-the-counter medications. By doing so, Defendant has violated the California Invasion of Privacy Act (“CIPA”), Cal. Penal Code § 631, and Pennsylvania’s Wiretapping and Electronic Surveillance Act (“WESCA”), 18 Pa. Cons. Stat. §§ 5701, *et seq.*

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

2. In or about May 2023, Plaintiff Doty visited the Website. During the visit, Defendant recorded Plaintiff Doty's electronic communications in real time, including Plaintiff Doty's mouse clicks, keystrokes, and prescription medications.

3. In or about May 2023, Plaintiff Ogden visited the Website. During the visit, Defendant recorded Plaintiff Ogden's electronic communications in real time, including Plaintiff Ogden's mouse clicks, keystrokes, and prescription medications.

4. Plaintiffs bring this action on behalf of themselves and a Class of all persons whose electronic communications were intercepted through the use of Defendant's wiretap on the Website.

THE PARTIES

5. Plaintiff Jalleh Doty is a resident of San Pedro, California and has an intent to remain there, and is therefore a citizen of California. In or about May 2023, prior to the filing of this lawsuit, Plaintiff Doty visited the Website, browsed over-the-counter medications, and refilled her prescription medications. Plaintiff Doty was in San Pedro, California when she visited the website. During the visit, Plaintiff Doty's electronic communications—including the URL values of the pages she visited, which showed which medications Plaintiff Doty browsed and refilled, as well as search terms she entered in the search bar—were read, accessed, learned, and intercepted in real time by Defendant QM through its software-as-a-service. Plaintiff Doty was unaware at the time that her electronic communications, including the information described above, were being intercepted in real-time and disclosed to QM, nor did Plaintiff Doty consent to the same.

6. Plaintiff Jeffrey Ogden is a resident of Selinsgrove, Pennsylvania and has an intent to remain there, and is therefore a citizen of Pennsylvania. In or about May 2023, prior to the filing of this lawsuit, Plaintiff Ogden visited the Website and refilled his prescription medications.

Plaintiff Ogden was in Selinsgrove, Pennsylvania when he visited the website. During the visit, Plaintiff Ogden’s keystrokes, mouse clicks, and other electronic communications—including the URL values of the pages he visited, which showed which medications Ogden refilled—were read, accessed, learned, and intercepted in real time by Defendant QM through its software-as-a-service. Plaintiff Ogden was unaware at the time that his electronic communications, including the information described above, were being intercepted in real-time and disclosed to QM, nor did Plaintiff Ogden consent to the same.

7. CVS Health Corporation owns and operates the Website.

8. Defendant Quantum Metric, Inc. is a Delaware corporation with its principal place of business at 10807 New Allegiance Drive, Suite 155, Colorado Springs, Colorado 80921.

9. QM is a marketing software-as-a-service (“SaaS”) company.

10. QM provides a feature called “Session Replay,” which is at issue here and described more fully below. At all relevant times here, CVS Health Corporation employed QM’s “Session Replay” product on the Website.

JURISDICTION AND VENUE

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

12. This Court has personal jurisdiction over Defendant because Defendant is headquartered in Colorado.

13. This Court is the proper venue for this action Pursuant to 28 U.S.C. § 1391 because Defendant resides in this District.

STATEMENT OF FACTS

I. OVERVIEW OF QM'S SERVICES

14. Defendant QM provides a software-as-a-service (“SaaS”) platform of the same name. The platform provides many features such as data analytics, AI analysis, and session replay. Each of these features is employed by CVS on the Website and is discussed in turn.

A. Session Replay

15. Most relevant to this action is QM’s “Session Replay” function. As QM describes Session Replay on its website:

Session replay is the reproduction of a user’s interactions on web or native mobile applications. Session replay captures things like mouse movements, clicks, typing, scrolling, swiping, tapping, etc. Session replay isn’t a recording of a user’s session. It’s a reproduction of the individual experience based on the changing state of their browser or application, with all of the underlying contextual user data.²

16. In more technical terms, a crucial component of every website is the Document Object Model (“DOM”), which “is the data representation of the objects that comprise the structure and content of a document on the web.”³ In other words, the DOM part of the foundation of any given website.

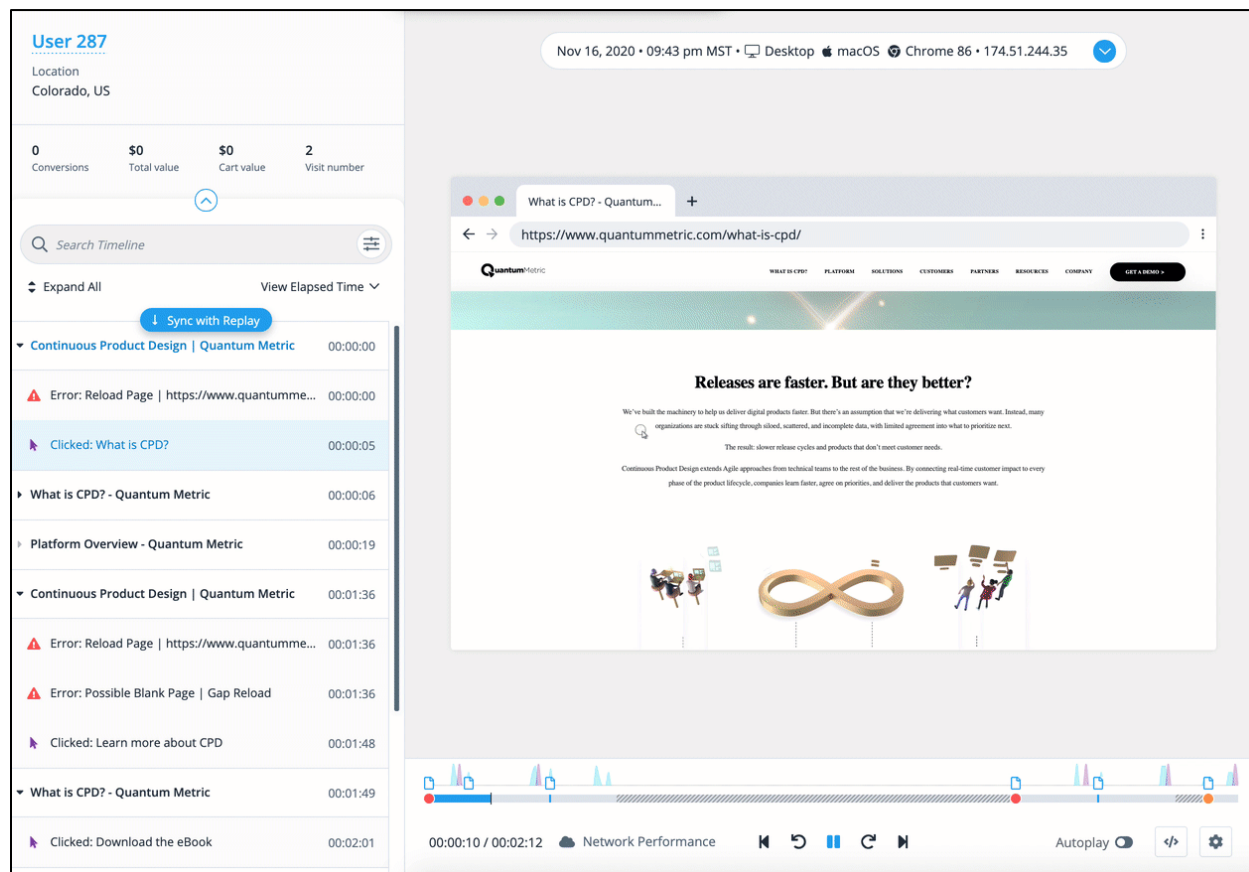
17. When a user interacts with a website—such as by clicking on particular item of interest or entering text into a search bar—the DOM is altered. Session replay services like QM’s “log[] every change made to the DOM, such as users entering or retrieving information, as an event. [They] then string[] these events together into a representation of each user’s individual session.”⁴

² SESSION REPLAY, <https://www.quantummetric.com/platform/session-replay/>

³ https://developer.mozilla.org/en-US/docs/Web/API/Document_Object_Model/Introduction.

⁴ <https://www.datadoghq.com/knowledge-center/session-replay/>.

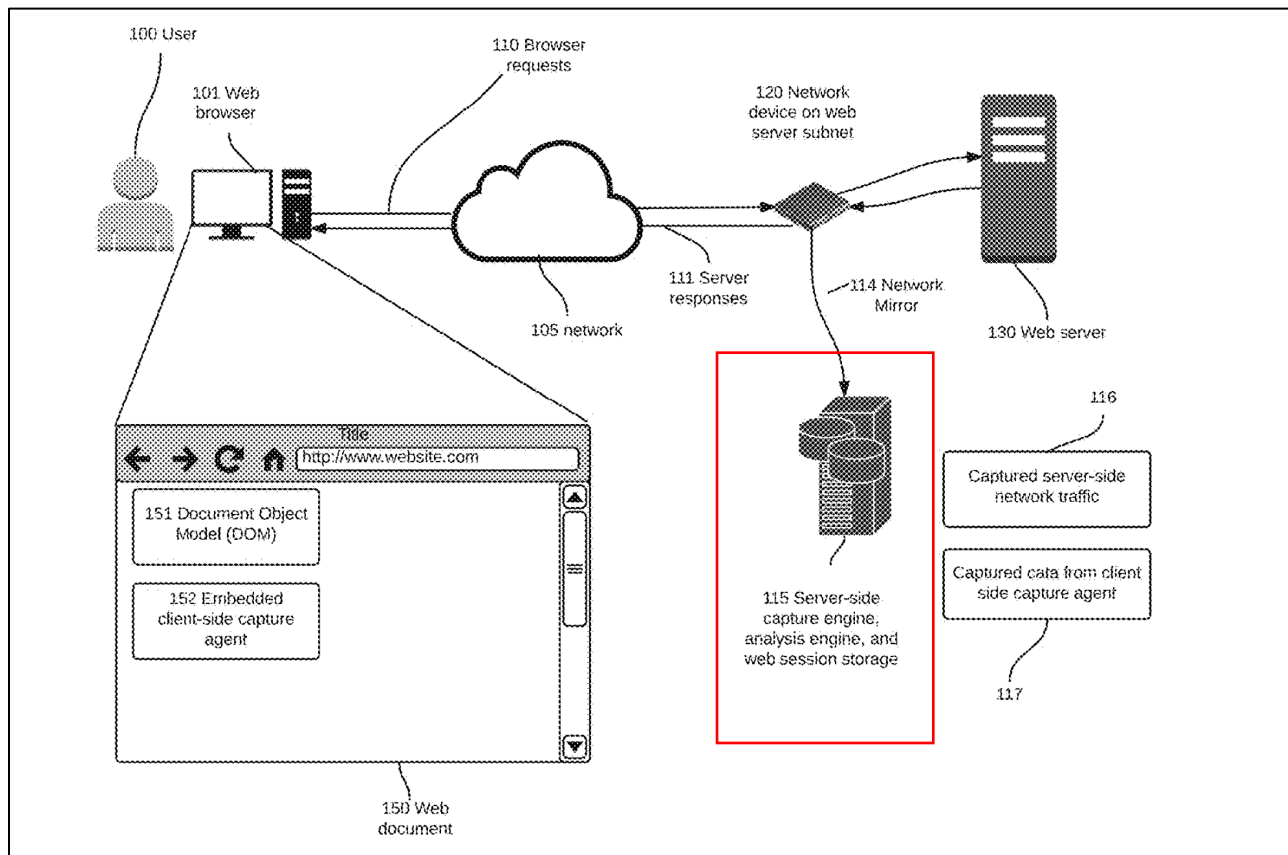
18. After capturing the event data (e.g., items clicked on or text entered)—as well as other elements such as how the website looks—session replay services like QM’s compile this information into a “video recording” of the user’s visit to the website. As a result, companies can “can pause, rewind, and fast-forward the session (just like a YouTube video) to watch how a user interacts with a website or mobile app”⁵:



19. The word “replay” is also a bit of a misnomer. The changes to the DOM (i.e., the user’s interactions with the website) are captured and transmitted to the session replay provider (i.e., QM) “at hyper-frequent intervals, often just milliseconds apart.” See *Price v. Carnival Corp.*, 2024 WL 221427, at *5 (S.D. Cal. Jan. 19, 2024). Thus, the capturing and reading of user information occurs in real time and contemporaneously with the communication.

⁵ <https://www.quantummetric.com/enterprise-guide-to-session-replay/#h1>.

20. QM's patent is illustrative of this contemporaneous interception. When a user communicates with a website (in the form of interactions like clicking items of interest or entering search terms), that information is transmitted to a web server. But, along the way, the "server-side capture engine" (QM's service) intercepts those communications. QM's service also captures communications being sent back from the website to the user:



Accurate And Efficient Recording Of User Experience, GUI Changes And User Interaction Events On A Remote Web Document, U.S. Patent No. 10,146,752, at fig. 1 (issued Dec. 4, 2018)

21. Because QM's session replay service operates in the same manner as alleged above, QM's session replay service suffers from the same privacy flaws as its competitors. As an article from the Center for Information Technology Policy at Princeton University found:

the extent of data collected by these services far exceeds user expectations ... text typed into forms is collected before the user submits the form, and precise mouse movements are saved, all without any

visual indication to the user. This data can't reasonably be expected to be kept anonymous.⁶

22. As the article goes on to note, “[c]ollection of page content by third-party replay scripts may cause *sensitive information such as medical conditions*, credit card details and other personal information displayed on a page to leak to the third-party as part of the recording,” which “may expose users to identity theft, online scams, and other unwanted behavior.”⁷

23. Sensitive user information may be leaked for a multitude of reasons, including but not limited to the fact that (i) “[a]utomated redaction is imperfect; fields are redacted by input element type or heuristics, which may not always match the implementation used by publishers (*e.g.*, information may be redacted when a form field auto-completes, but not when it is manually entered); (ii) page content may not be redacted, even if user inputs are; and (iii) websites operators must manually configure and label personal information to be redacted, which does not always occur.”⁸

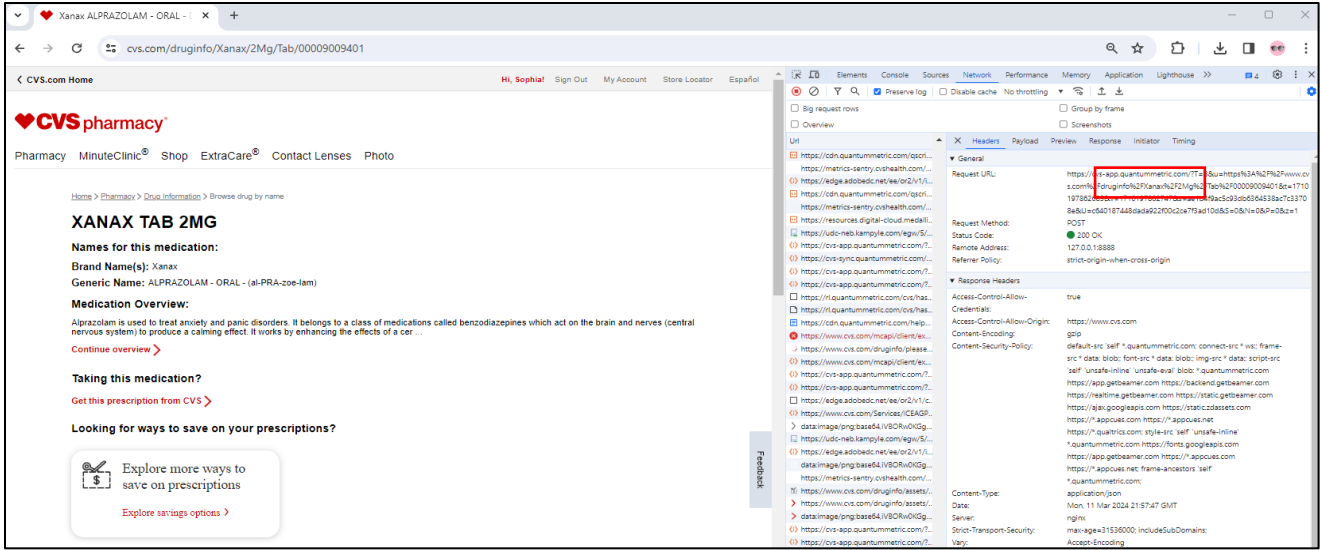
24. QM is no exception to this. Each website operator must manually select whether information should be captured, not captured, or encrypted.⁹ This is an imperfect process. For instance, and as alleged in more detail below, on CVS’s Website, the full names of prescription medications and their dosages purchased by users are being captured unencrypted by QM via the URL value:

⁶ <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/>.

⁷ *Id.* (emphasis added).

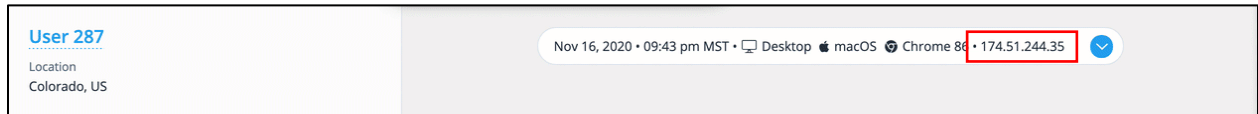
⁸ *Id.*

⁹ <https://www.quantummetric.com/platform/data-privacy-security/>.



25. Further, this information is not anonymized, as a user is logged into her CVS account while browsing the Website and QM is capturing the name of the user’s account.

26. In addition, QM’s Session Replay feature captures other identifiers, including a user’s IP address:



27. The IP address is a unique identifier for a device, which is expressed as four sets of numbers separated by periods (e.g., 192.168.123.132). The first two sets of numbers indicate what network the device is on (e.g., 192.168), and the second two sets of numbers identify the specific device (e.g., 123.132).

28. Thus, the IP address enables a device to communicate with another device—such as a computer’s browser communicating with a server—and the IP address contains geographical location.

29. Through an IP address, the specific device’s state, city, and zip code can be determined.

30. Much like a telephone number, an IP address is a unique numerical code associated with a specific internet-connected device. Thus, knowing a user’s IP address—and therefore

geographical location—”provide[s] a level of specificity previously unfound in marketing.”¹⁰

31. An IP address allows advertisers to (i) “[t]arget [customers by] countries, cities, neighborhoods, and ... postal code”¹¹ and (ii) “to target specific households, businesses[,] and even individuals with ads that are relevant to their interests.”¹² Indeed, “IP targeting is one of the most targeted marketing techniques [companies] can employ to spread the word about [a] product or service”¹³ *because* “[c]ompanies can use an IP address ... to personally identify individuals.”¹⁴

32. For example, businesses who are trying to reach college-aged demographics can target devices on college campuses by sending advertisements to IP addresses associated with college-wide Wi-Fis.¹⁵ Or, for a job fair in specific city, companies can send advertisements to only those in the general location of the upcoming event.¹⁶

33. In addition to “reach[ing] their target audience with greater precision,” businesses are incentivized to use a customer’s IP address because it “can be more cost-effective than other forms of advertising.”¹⁷ “By targeting specific households or businesses, businesses can avoid

¹⁰ *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA, <https://www.accudata.com/blog/ip-targeting/>.

¹¹ *Location-based Targeting That Puts You in Control*, CHOOZLE, <https://choozle.com/geotargeting-strategies/> (last visited April 17, 2024).

¹² Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29, 2023), <https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf>.

¹³ *IP Targeting: Understanding This Essential Marketing Tool*.

¹⁴ Trey Titone, *The future of IP address as an advertising identifier*, AD TECH EXPLAINED (May 16, 2022), <https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/>.

¹⁵ *See, e.g., IP Targeting: Understanding This Essential Marketing Tool*, *supra* note 1.

¹⁶ *See, e.g., Personalize Your Website And Digital Marketing Using IP Address*, GEOFLI, <https://geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-marketing-campaigns>.

¹⁷ Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*.

wasting money on ads that are unlikely to be seen by their target audience.”¹⁸

34. In addition, “IP address targeting can help businesses to improve their overall marketing strategy.”¹⁹ “By analyzing data on which households or businesses are responding to their ads, businesses can refine their targeting strategy and improve their overall marketing efforts.”²⁰

35. In short, QM’s Session Replay service allows QM to capture, read, and learn every communication (*e.g.*, text entered, medications purchased, information clicked on) between a CVS user and the Website in real time, and in a deanonymized manner.

B. Data Analytics, AI, And Partner Integrations

36. Beyond capturing and reading user’s personal information, QM also has the capability to analyze the captured information with a sophisticated suite of services—including AI—and further disclose captured user information to other third parties.

37. Defendant provides its partners, like CVS, with analytics, including behavioral metrics, technical metrics, and business metrics. Defendant also collects “over 300 audience dimensions such as browser, device type, and location.”²¹

38. The behavioral metrics Defendant collects includes “clicks, taps, scrolls, long running spinners, scroll depth, form submits, back button usage, page views, typed text, frustration signals, and more.”²²

39. Defendant’s website touts its autocapture feature, telling customers to “leverage the

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ *Id.*

²¹ <https://www.quantummetric.com/platform/data-capture-and-activation/>

²² *Id.*

power of Quantum Metric’s autocapture for every user interaction – swipe, click, scroll, API response, page view, and more – to enhance and improve its understanding of your data.”²³

40. Moreover, Defendant’s Feliz AI tool has the capacity to “automatically summarize the thousands of data points collected in a user session and consolidates the session timeline into a short, readable summary.”²⁴

41. Defendant’s customers, like CVS, incorporate these services into their sites.

42. Defendant’s offered services also utilize the assistance of third parties, including but not limited to, Google Analytics, Adobe Analytics, Salesforce, AppDynamics, and more.²⁵ Defendant thus shares users’ information with these third parties.

43. For example, Defendant’s website explains customers can “enrich Google Analytics with digital experience metrics and deep links into the Quantum Metric platform.” This allows customers to receive “enhanced learning” including “a complete overview of every user session.”²⁶ Defendant provides the same explanation for its use of Adobe Analytics.²⁷

44. Because QM has the capability to “capture[], store[], and interpret[] [] real-time data,” it is not like a tape recorder or “tool” used by one party to record another. *See Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021) (finding plaintiff sufficiently alleged Quantum Metric was akin to “an eavesdropper standing outside the door”). Instead, QM— a separate and distinct third-party entity from the parties to the conversation (Plaintiffs and Class

²³ <https://www.quantummetric.com/platform/platform-intelligence/>

²⁴ *Id.*

²⁵ <https://www.quantummetric.com/partners/partner-network/#technology,customer-experience,performance-monitoring,marketing-analysis,experimentation>.

²⁶ <https://www.quantummetric.com/partners/integration-google-analytics/>

²⁷ <https://www.quantummetric.com/partners/integration-adobe-analytics/>

Members, on the one and, and CVS, on the other)—eavesdrops upon, records, extract data from, and analyzes a conversation to which it was not a party. This is because QM itself is collecting the content of any conversation. That data is then analyzed by QM in the manner alleged above before being provided to any entity that was a party to the conversation (like CVS).

II. QM CAPTURES THE PERSONAL INFORMATION OF CVS.COM USERS

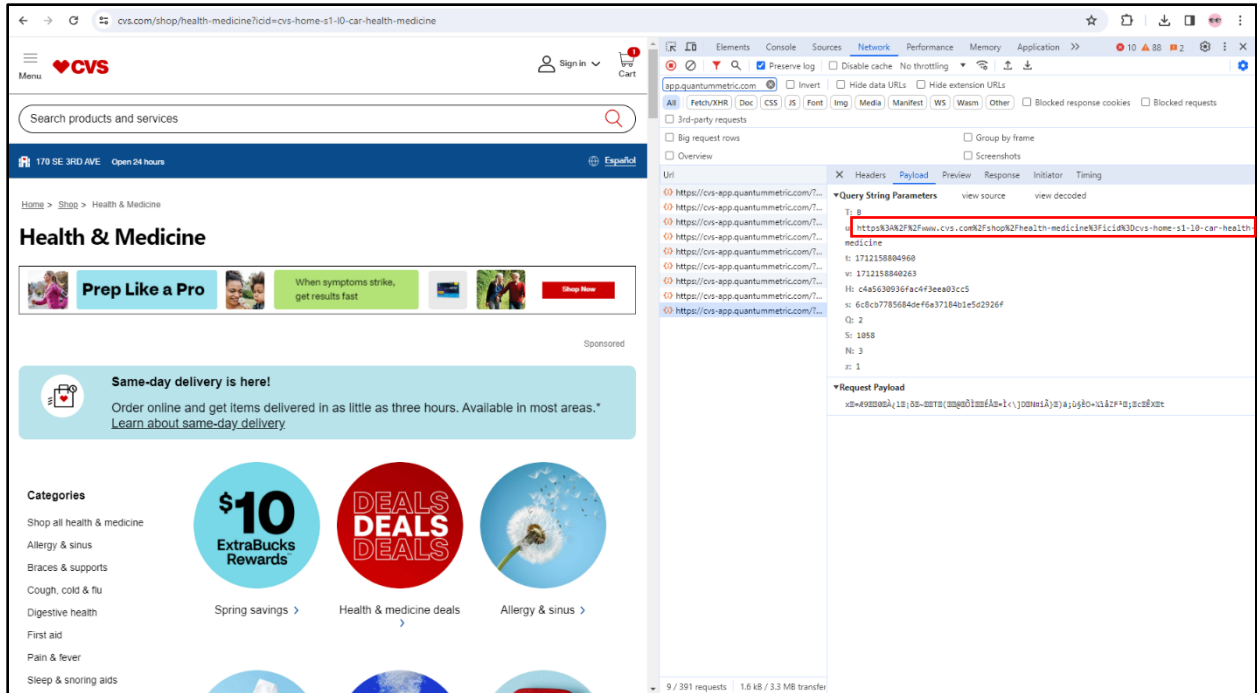
45. QM business model involves providing the services outlined above for a fee to website owners. One of QM’s featured clients is CVS:



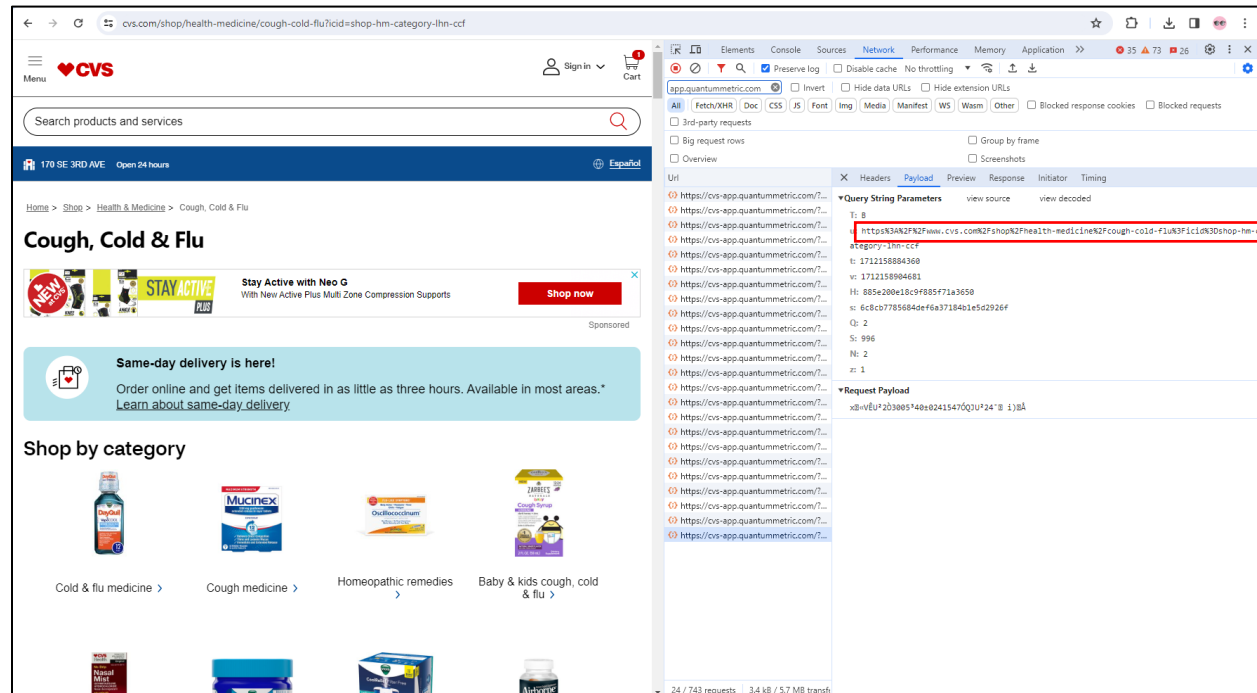
46. QM operates on CVS’s Website in the manner described above. Thus, on CVS’s Website, QM captures website users’ electronic communications in real-time through its Session Replay feature, and then has the capability to analyze those communications and divulge them to other third parties.

47. QM’s software-as-a-service begins operating as soon as a user accesses the Website. Thus, users are not on notice of QM’s wiretapping, nor do users provide their consent to the same.

48. Contrary to its representations, QM captures a host of sensitive medical information on the Website, and in a non-anonymized manner. For instance, if a user clicks on the “Health and Medicine” category on the Website, QM captures this electronic communication via the URL value:

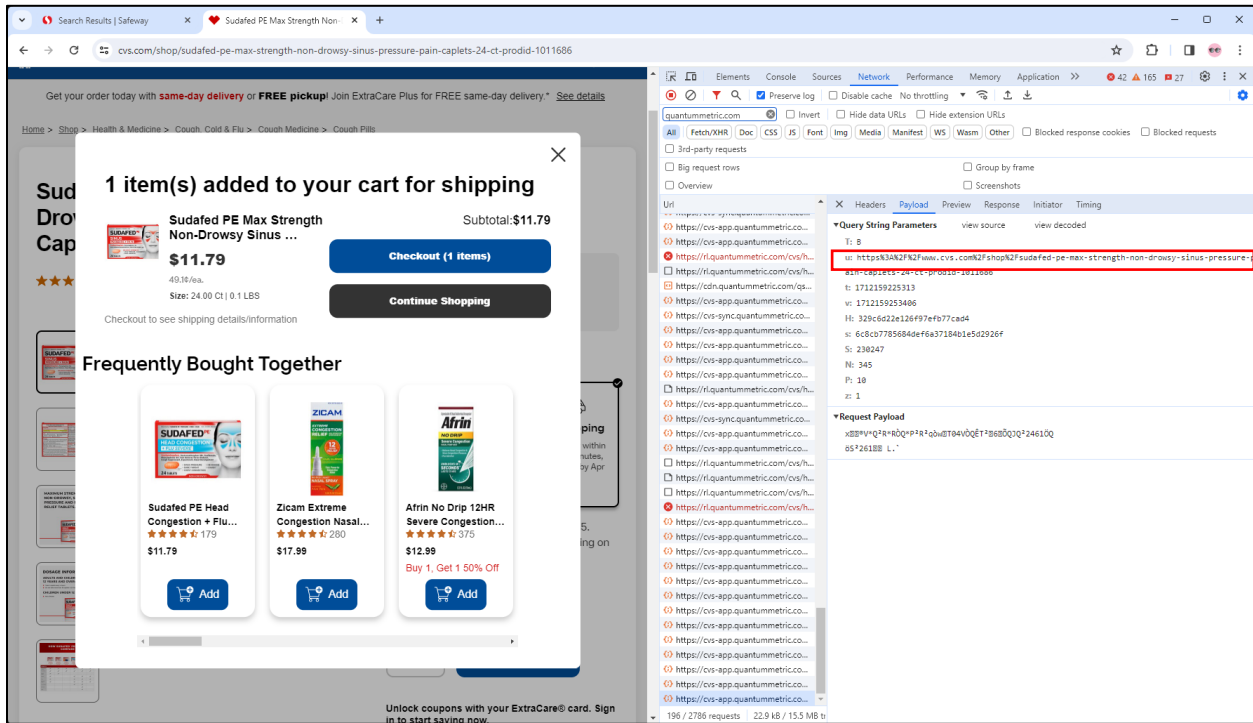


49. If a user then searches for or clicks on specific medications (e.g., “Cough, Cold & Flu”), QM will capture those search terms or the medication category via the URL value. The latter is pictured below:

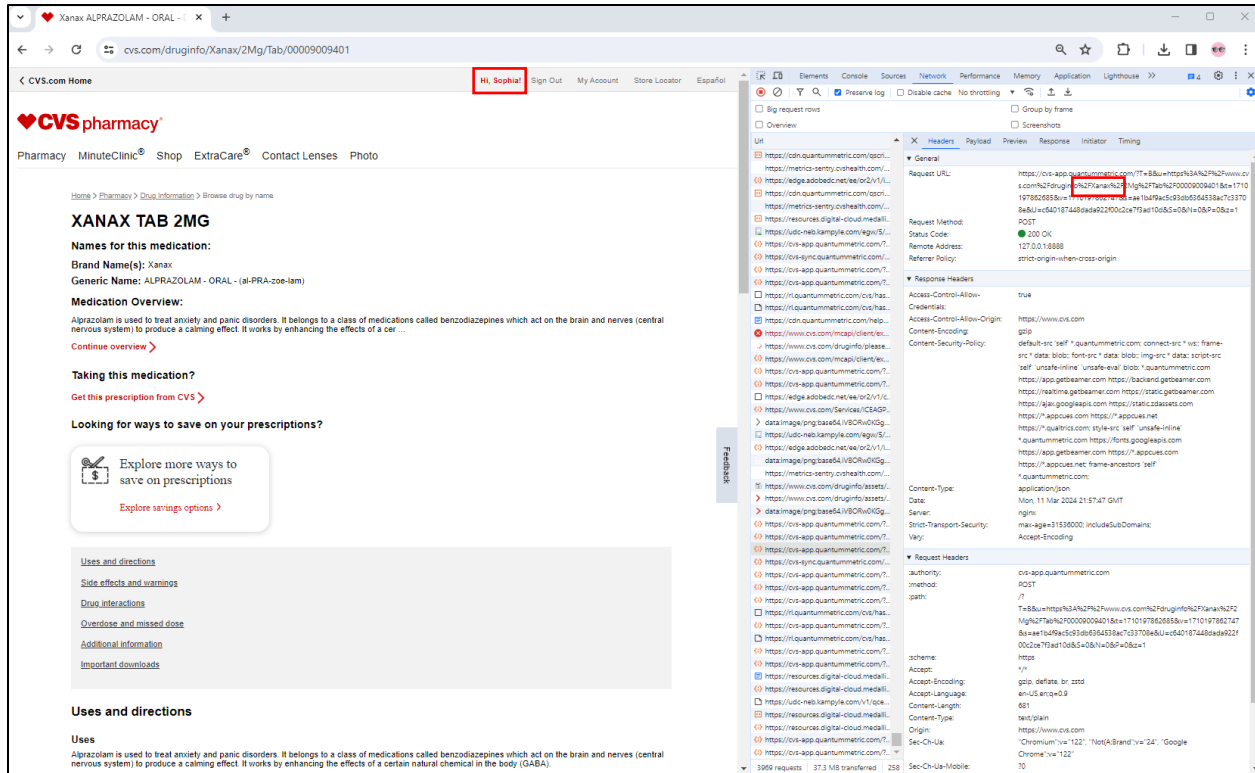


50. If a user adds a specific medication to their cart, QM captures this electronic

communication, with the URL value captured by QM disclosing the specific medication selected. In the below screenshot, for example, QM is learning that a user is adding Sudafed to their cart:



51. QM's wiretapping does not stop at over-the-counter medications. If a user goes to refill their prescriptions, QM will capture this electronic communication, with the URL value divulging the name of the specific medication the user is seeking to refill. Crucially, QM is also capturing the name of the user's account and IP address, meaning the information captured is in a non-anonymized format:



52. As alleged above, once QM captures these electronic communications, it has the capability to analyze the electronic communications of Website users and further divulge those communications to other third parties, such as Google and Adobe. In addition, QM has the capability to use aggregated Website user data to “collect and analyze data and other information relating to the provision, use and performance of various aspects of the Quantum Service and related systems and technologies (including, without limitation, information concerning Customer Data and data derived therefrom), and Quantum will be free (during and after the Term) to use such information and data to improve and enhance the Quantum Technology and for other development, diagnostic and corrective purposes in connection with the Quantum Service and other Quantum offerings.”²⁸

53. As currently employed on the Website, QM’s service functions as a wiretap.

²⁸ <https://iam.quantummetric.com/terms-and-conditions>.

III. EXPERIENCES OF PLAINTIFFS

54. In or about May 2023, Plaintiffs visited CVS.com and refilled their prescriptions. Plaintiff Doty also searched for various medications on the Website.

55. QM was employed by CVS on the Website during Plaintiffs' visits. Thus, when Plaintiffs communicated with the Website, QM captured those electronic communications, including the pages viewed/URL values of those pages and the search terms entered by Plaintiff Doty. The electronic communications captured by QM revealed the contents of Plaintiffs' communications—specifically, the medications searched for or refilled by Plaintiffs.

56. QM also captured information that divulged Plaintiffs' identities, including but not limited to Plaintiffs' user account names and IP addresses.

57. QM's wiretapping of Plaintiffs' electronic communications began the moment Plaintiffs accessed the Website.

58. Neither CVS nor QM asked Plaintiffs whether they consented to being wiretapped by QM. Plaintiffs were never explicitly told that their electronic communications were being wiretapped by QM, nor did CVS nor QM procure Plaintiffs' prior consent to the wiretapping.

59. Plaintiff Doty was in California when she accessed the Website through her internet browser. Upon having her browser access the Website in California, QM's service instructed the browser in California to send electronic communications directly to it from the California location of the browser to QM's servers.

60. Plaintiff Ogden was in Pennsylvania when he accessed the Website through his internet browser. Upon having his browser access the Website in Pennsylvania, QM's service instructed the browser in Pennsylvania to send electronic communications directly to it from the Pennsylvania location of the browser to QM's servers.

CLASS ACTION ALLEGATIONS

61. Plaintiff Doty seeks to represent a class of all California residents who visited the Website while in California, and whose electronic communications were intercepted or recorded by QM during the statute of limitations period (the “California Class”).

62. Plaintiff Ogden seeks to represent a class of all Pennsylvania residents who visited the Website while in Pennsylvania, and whose electronic communications were intercepted or recorded by QM during the statute of limitations period (the “Pennsylvania Class”) (together with the California Class, the “Classes”).

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

64. Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to, whether Defendant violated CIPA § 631; whether Defendant violated the WESCA; and whether class members are entitled to actual and/or statutory damages for the aforementioned violations.

65. The claims of the named Plaintiffs are typical of the claims of the Class because the named Plaintiffs, like all other Class Members, visited the Website and had their electronic communications intercepted by QM through QM’s service.

66. Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class Members they seek to represent, they have retained

competent counsel experienced in prosecuting class actions, and they intend to prosecute this action vigorously. The interests of Class Members will be fairly and adequately protected by Plaintiffs and their counsel.

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

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

68. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

69. Plaintiff Doty brings this claim individually and on behalf of the members of the proposed California Class against Defendant.

70. The California Legislature enacted the CIPA to protect certain privacy rights of California citizens. The legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications ... has created a

serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.” Cal. Penal Code § 630.

71. The California Supreme Court has repeatedly stated an “express objective” of CIPA is to “protect a person placing or receiving a call from a situation where the person on the other end of the line *permits an outsider to tap his telephone or listen in on the call.*” *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985) (emphasis added)

72. Further, as the California Supreme Court has held in explaining the legislative purpose behind CIPA:

While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its *simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device.*

As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements.

Ribas, 38 Cal. 3d at 360-61 (1985) (emphasis added; internal citations omitted).

73. 64. CIPA § 631(a) imposes liability for “distinct and mutually independent patterns of conduct.” *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under CIPA § 631(a), a plaintiff need only establish that the defendant, “by means of any machine, instrument, contrivance, or in any other manner,” does any of the following:

Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,

Or

Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in

transit or passing over any wire, line or cable or is being sent from or received at any place within this state,

Or

Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,

Or

Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

74. Section 631(a) is not limited to phone lines, but also applies to “new technologies” such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new technologies” and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs “electronic communications”); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook’s collection of consumers’ Internet browsing history); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) (“Though written in terms of wiretapping, Section 631(a) applies to Internet communications.”).

75. QM’s software-as-a-service is a “machine, instrument, contrivance, or ... other manner” used to engage in the prohibited conduct at issue here.

76. QM is a “separate legal entity that offers ‘software-as-a-service’ and not merely a passive device.” *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Accordingly, QM was a third party to any communication between Plaintiff Doty and California Class Members, on the one hand, and the CVS Website, on the other. *Id.* at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023); *Yoon*, 549 F. Supp. 3d at 1081.

77. At all relevant times, QM willfully and without the consent of all parties to the communication, or in any unauthorized manner, read or attempted to read or learn the contents or meaning of electronic communications of Plaintiff Doty and California Class Members, on the one hand, and the CVS Website, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

78. Plaintiff Doty and California Class Members did not provide their prior consent to QM's intentional access, interception, reading, learning, recording, and collection of Plaintiff Doty's and California Class Members' electronic communications. *Javier v. Assurance IQ, LLC*, 2023 WL 114225, at *2 (N.D. Cal. Jan. 5, 2023). (“[W]e conclude that the California Supreme Court would interpret Section 631(a) to require the prior consent of all parties to a communication.”).

79. The wiretapping of Plaintiff Doty and California Class Members occurred in California where Plaintiff Doty and California Class Members accessed the Website and where QM's session replay feature routed Plaintiffs' and Class Members' electronic communications to QM's own servers. *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 131 (3d Cir. 2022).

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

COUNT II
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 632

81. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

82. Plaintiff Doty brings this claim individually and on behalf of the members of the proposed California Class against Defendant.

83. California Penal Code § 632 prohibits an entity from:

intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio.

84. Defendant’s software-as-a-service feature is an “electronic amplifying or recording device.”

85. At all times, the communications between Plaintiff Doty and California Class Members, on the one hand, and CVS.com, on the other, were confidential.

86. At all relevant times, QM intentionally used the session replay feature to eavesdrop and record the confidential communications of Plaintiff Doty and California Class Members, on the one hand, and CVS.com, on the other.

87. When communicating with CVS, Plaintiff Doty and California Class Members had an objectively reasonable expectation of privacy. Plaintiff Doty and California Class Members did not reasonably expect that anyone other than CVS would be on the other end of the confidential communications, nor that other third-party entities like QM would intentionally use an electronic amplifying or recording device to eavesdrop upon and record the confidential communications of Plaintiff Doty and California Class Members. Indeed, Plaintiff Doty and California Class Members each communicated medical-related information to CVS, which enhances their reasonable expectation of privacy because such sensitive information should not be disclosed to nor intercepted by third parties like QM.

88. Plaintiff Doty and California Class Members did not provide their prior consent to QM’s intentional access, interception, reading, learning, recording, and collection of Plaintiff Doty’s and California Class Members’ electronic communications.

89. The wiretapping of Plaintiff Doty and California Class Members occurred in California where Plaintiff Doty and California Class Members accessed the Website and where QM's session replay feature routed Plaintiff Doty's and California Class Members' electronic communications to QM's own servers. *Popa*, 52 F.4th at 131.

90. Pursuant to Cal. Penal Code § 637.2, Plaintiff Doty and California Class Members have been injured by the violations of CIPA § 632(a), and seek statutory damages of \$5,000 for each of Defendant's violations of CIPA § 632(a).

COUNT III
**Violation Of The Pennsylvania Wiretapping And Electronic Surveillance Act,
18 Pa. Cons. Stat. § 5701, et seq.**

91. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

92. Plaintiff Ogden brings this claim individually and on behalf of the members of the proposed Pennsylvania Class against Defendant.

93. The WESCA 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(1)-(3).

94. 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).

95. At all relevant times, through its session replay feature, Defendant intentionally intercepted, used, and disclosed the electronic communications between Plaintiff Ogden and Pennsylvania Class Members on the one hand, and CVS.com on the other hand.

96. Plaintiff Ogden and Pennsylvania Class Members did not provide their prior consent to having their electronic communications intercepted by Defendant.

97. Plaintiff Ogden and Pennsylvania Class Members had a justified expectation under the circumstances that their electronic communications would not be intercepted by Defendant. Plaintiff Ogden and Pennsylvania Class Members reasonably believed these communications would only be accessed by the Website, and not by a third party like QM. Further, in this case, Plaintiff Ogden and Pennsylvania Class Members were communicating sensitive medical-related information that a third party like QM had no business acquiring.

98. The wiretapping of Plaintiff Ogden and Pennsylvania Class Members occurred in Pennsylvania, where Plaintiff Ogden and Pennsylvania Class Members accessed the Website and where QM routed Plaintiff Ogden's and Pennsylvania Class Members' electronic communications to QM's own servers. *Popa*, 52 F.4th at 131.

99. Plaintiff Ogden and Pennsylvania Class Members seek all relief available under 18 Pa. Cons. Stat. § 5725(a).

PRAYER FOR RELIEF

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

- (a) For an order certifying the Classes under Rule 23, naming Plaintiffs as the representatives of the Class, respectively, and naming Plaintiffs' attorneys as Class Counsel to represent the Class;
- (b) For an order declaring that the Defendant's conduct violates the statutes referenced herein;
- (c) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;
- (d) For compensatory, punitive, and statutory damages in amounts to be determined by the Court and/or jury;
- (e) For prejudgment interest on all amounts awarded;
- (f) For an order of restitution and all other forms of equitable monetary relief;
- (g) For injunctive relief as pleaded or as the Court may deem proper; and
- (h) For an order awarding Plaintiffs and the Class their reasonable attorneys' fees and expenses and costs of suit.

DEMAND FOR TRIAL BY JURY

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

Dated: April 25, 2024

Respectfully submitted,

BURSOR & FISHER, P.A.

By: /s/ Max S. Roberts
Max S. Roberts

Philip L. Fraietta (*Admission Forthcoming*)
Max S. Roberts
Caroline C. Donovan (*Admission Forthcoming*)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com
mroberts@bursor.com
cdonovan@bursor.com

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Software Company Quantum Metric Under Fire for Alleged Tracking of CVS Website Users' Online Activity](#)
